AUSTRALIAN EDITION

DIGITAL ARMAGEDDON 2000

How to stop the Millennium bug before it stops your business

JOHN GOOD

DIGITAL
ARMAGEDDON
2000

DIGITAL ARMAGEDDON 2000

How to stop the Millennium bug before it stops your business

JOHN GOOD

PRENTICE HALL

Sydney New York Toronto Mexico New Delhi
London Tokyo Singapore Rio de Janeiro

© 1998 by Prentice Hall Australia Pty Ltd

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the written permission of the publisher.

Acquisitions Editor: Jane Ogilvie
Production Editor: Esperanza Egan
Copy Editor: Robyn Flemming
Cover and internal designed by Jack Jagtenberg, Stanmore, NSW
Cover illustration by Steven Bray, Petersham, NSW
Typeset by The Type Group, Fairy Meadow, NSW
Printed in Australia by Australian Print Group, Victoria

1 2 3 4 5 02 01 00 99 98

ISBN 0 7248 0318 1

National Library of Australia
Cataloguing-in-Publication Data

Good, John.
Digital Armageddon 2000: how to stop the millenium bug
before it stops your business.

ISBN 0 7248 0318 1.

1. Year 2000 date conversion (Computer systems). I. Title.

005.16

Prentice Hall of Australia Pty Ltd, *Sydney*
Prentice Hall, Inc., *Upper Saddle River, New Jersey*
Prentice Hall Canada, Inc., *Toronto*
Prentice Hall Hispanoamericana, *SA, Mexico*
Prentice Hall of India Private Ltd, *New Delhi*
Prentice Hall International, Inc., *London*
Prentice Hall of Japan, Inc., *Tokyo*
Simon & Schuster (Asia) Pte Ltd, *Singapore*
Editora Prentice Hall do Brasil Ltda, *Rio de Janeiro*

PRENTICE HALL

A division of Simon & Schuster

CONTENTS

Acknowledgments **vii**
Disclaimer **viii**
How to use this book **ix**
Introduction **x**

1 The problem and why it matters **1**
2 How it happened **7**
3 How you may be affected **13**
4 'Year 2000 ready' or 'compliant' **17**
5 Conventional computer systems **19**
6 Personal computers **25**
7 Embedded electronic chips **31**
8 Your business and technical suppliers **37**
9 Your customers: Your risk from them and their risk from you **41**
10 Infrastructures and your industry **45**
11 The global impact and the effect on Australia **49**
12 The legal aspects **57**
13 Who is accountable for protecting your organisation? **67**
14 How to beat the looming skill shortage **71**
15 What should you do now? **73**
16 Where to obtain further help **85**

Appendix: Review your organisation **87**

ACKNOWLEDGMENTS

I should like to acknowledge the encouragement and contributions of a number of people in the writing of this book. Thanks are due first to Shoal Bay Press in New Zealand and Prentice Hall of Australia for suggesting that a book of this type might be needed and for inviting me to write it.

The ideas of a number of people are acknowledged in the text. Craig Jones, who is a practising barrister and solicitor, contributed the content of Chapter 12. My colleagues at Azimuth Consulting Ltd in Australia and New Zealand have contributed in all sorts of ways. In particular, Liz Westbrooke, who helped me to establish the Azimuth Year 2000 Competency Centre, contributed much of the material for Chapter 6. Laurence Millar read a late draft of the book, took it by the scruff of the neck and improved its clarity no end. David Niven has contributed a number of suggestions using his experience of the Australian Year 2000 scene. Alex Frater and Bryce Pottinger made useful comments about the final draft.

Thanks also to numerous clients. None of them is directly referred to in the book, but their experience has helped me tremendously in developing my views on how to handle this unprecedented problem. The views expressed in the book, and the responsibility for them, are mine alone.

My greatest debt, as always, is to my wife, Val Lindsay, who has encouraged, contributed to and accommodated my doing this extra task alongside the demands of our young family and her academic career—and allowed me to use her e-mail address!

John Good
March 1998, Browns Bay
Auckland, New Zealand
E-mail: 100017.741@compuserve.com

DISCLAIMER

This book has been produced to provide general guidance and advice with regard to the Year 2000 problem. While it aims to give practical advice to the reader and to suggest good practice for dealing with the problem, the material is of necessity general in nature. Readers will therefore be entirely responsible for their own actions with regard to the Year 2000 problem within their organisations and for the consequences of such actions. Nothing in this book constitutes legal or professional advice. Always consult a lawyer or other professional person on any specific problem or matter.

HOW TO USE THIS BOOK

This book is written, as far as possible, in non-technical language. It is intended to be an easy read. You, the reader, are intended to interact with the book, using it as a manual.

Chapters 1 to 3 provide an overview of the problem and the many forms that it can take. Don't skip these. They and the following chapters include some action points and questions for you to address with regard to your own situation. Space is provided in the appendix at the back of the book for this purpose.

Chapter 4 defines what we mean by 'Year 2000 ready'.

Chapters 5 to 11 deal with different aspects of the problem, providing some examples.

Chapter 12 looks at the legal issues, **Chapter 13** at identifying who is accountable for dealing with the problem and **Chapter 14** at the resource implications. Again, make your own notes in the space provided in the appendix. Your complete set of responses will form a very useful first step towards ensuring that you manage your own Year 2000 exposure in an informed, comprehensive and successful way.

Chapter 15 builds from this first step and explains how to diagnose your own Year 2000 problems, assess your risk, decide what to do about it and then manage that remedial work.

Chapter 16 contains some suggestions on where to look for further information about the topic.

INTRODUCTION

This book is for people who are not particularly well versed in technical matters but who have heard that there is a problem to do with the Year 2000 and computers. They want to find out if the problem could affect them and what they should do if it does—but they don't quite know where to start.

This is not an expert book—there are no real experts yet in dealing with this problem. Real expertise will be available around the year 2001 when we have had a thorough chance to see what has worked and what hasn't! Rather, it is based on the shared experience of many people who have dealt with computers and organisations over many years and on a reading of the views of some of the leading figures who are now working on Year 2000 issues. It also reflects my experience working with the staff of organisations who are trying to assess and solve their Year 2000 problems.

It is not a book for technical people who are trying to fix the problem. It is written for people who don't read the computer pages in the newspapers. It is about assessing the extent of your Year 2000 problems (you may find you don't have any) and managing your way through. It won't teach you to fix them—you'll get someone else to do that if you need to.

Above all, it is a book written with Australians in mind. Australia has a great opportunity, for reasons that I will explain, to become ready for the Year 2000 before some of the major players have done so. But Australia has been slow to respond. Only recently has this issue been getting media coverage outside the computer pages. We are perhaps nine months behind the United States and the United Kingdom—any further delay and we'll be in the same mess as they are likely to find themselves in.

We have to understand that the Year 2000 problem will be no respecter of type or scale of organisation. It can be an equally major issue for the chief executive officer of Telstra and the owner of the corner delicatessen; for the Commonwealth Department of Finance and for a one-person architectural draughting practice. And they all share the same fixed deadline: 1 January 2000; earlier if the problem strikes before then, as it well may.

The Year 2000 is likely to become a legal minefield for the unwary. This book does not purport to provide legal advice. However, Craig Jones of the legal firm Maude & Miller specialises in this area and has provided a summary of the key legal issues in Chapter 12.

The Year 2000 problems in your organisation may need a great deal of effort to fix or evade, so time is of the essence. Until you have assessed the extent of your Year 2000 problems, any delay is dangerous. There is much to be done, and this book will show you where to start.

1 CHAPTER

The problem and why it matters

This book is about a technical problem that has the capacity to cause global havoc as we move from this century to the next. It is a problem that exists in billions of locations in scores of millions of computer systems and items of equipment around the world. It is a real problem, not a scare story.

In Australia, even though the problem is not likely to be as severe or widespread as in the larger developed nations, it is unlikely that there will be any organisation not affected by it in some way. It is equally unlikely that all organisations will survive its impact. Fortunately, although we are starting too late for comfort here in Australia, we still have time to work out the best way to handle the threat. But first we have to accept that this is a real enemy.

What's the problem?

The enemy goes under various names: the Year 2000 Issue, the Millennium Bomb, Y2K, and so on. We'll just call it the Year 2000 problem. We are told that it always helps to know your enemy, so let's start by learning a little about the nature of this one. It all hinges on two things: the fact that the most common item of information recorded in computers is (you guessed it!) a date, and their most common method of recording dates, called the two-digit year. This means instead of using four digits to record the year (1997), most computers use just the last two (97).

We humans often abbreviate the year in this way ourselves and this is fine because we can usually understand quite easily what we mean from the context. Computers have never been able to do that; they are programmed very precisely and will behave every time exactly the way they have been programmed. They are reliable but dumb!

Some homespun examples: my grandfather was born in 76 and my father in 05. I was born in 38 and I will retire in 08, if I last that long! These examples are entirely clear to us because we fill in the context for ourselves automatically. A computer dealing only in two-digit years won't do that, so it will presume that my grandfather is now 22, that I will retire three years after my father was born and that when I retire my age will be minus 30!

Now can you see the problem when computers using two-digit years start to deal with dates in 2000 and beyond? When computers have to move from 1999 to 2000, many of them will not be able to cope sensibly with a year whose value apparently is 99 less than the previous one. Time will seem to be going backwards! The computer will presume that 00 stands for 1900, 01 stands for 1901, and so on.

When will it strike?

We don't have to wait until 2000 to find real-life examples of the problem: in some situations it is occurring already. The Office of Government Information Technology (OGIT) reported to its Year 2000 subcommittees that the following problems had already been identified in Australia:

- A major bank in Sydney had all of its building and security systems running on a personal computer system which was not ready for the Year 2000. This would cause the building and lift systems to operate unpredictably after 2000.
- A major power plant in South Australia would be unable to monitor its generator control processes because chips installed throughout the plant would not be able to handle the transition to 2000.

- A hospital in Perth would be unable to use its dialysis equipment, which is used to keep some patients alive, because the machines would be unable to determine the correct date and would therefore presume that they needed long-overdue maintenance and would shut themselves down permanently.
- One of the major airlines was unable to award or track frequent flyer points for customers travelling after the Year 2000.

These mishaps occurred because the computer programs involved in each instance were having to deal with dates for the Year 2000 and beyond and could not do so sensibly because the years had been recorded as two digits and not four.

Organisations seem to be disinclined to reveal that they have experienced Year 2000 problems already. However, industry surveys in 1997 suggested that around a quarter of organisations had already experienced Year 2000 problems. These early manifestations arise in an organisation when one of its computer programs first has to deal with a year beyond 1999 that is represented as two digits.

What will happen?

When the problem strikes, almost anything may happen. It could be something simple, like '1900' appearing in the printed date on a letter meant to be dated 2000. In some cases the computer will just stop and do nothing more. At worst, it will carry on and do something really silly—maybe lots of silly things. Just possibly the results won't matter, but most likely they will. An example of what can happen when computer equipment stops occurred at midnight on 31 December 1996 at the Comalco company's aluminium smelters in Tasmania and New Zealand. The smelters are operated by hundreds of process control computers. All of these stopped simultaneously because they had not been provided with a code to handle the situation when they arrived at the end of the 366th day of a leap year! The resulting chaos caused some smelter pots to become unmanageable. Expensive damage resulted. (This was a Leap Year problem, not a Year 2000 problem, but it is a good example of the kind of thing that may happen on 1 January 2000, all the same.) There are two points to make about this:

1 The process controllers stopped in this case because they could not continue. They did not ramble on executing code erroneously and possibly producing even more havoc.

2 This was apparently a single problem[1] replicated hundreds of times. As such, this would have been much easier to diagnose—and probably also to fix—than a series of different problems on different types of computers.

The all-too-realistic nightmare prospect for organisations that don't take this problem seriously is this: many different problems all kick in at midnight on 31 December 1999 and become apparent over the following hours and days. This could easily result in a heap of problems too difficult for the organisation to get its collective mind around. And, until you understand these problems, you cannot fix them.

As we explain in the next chapter, the two-digit year method has been used since the earliest days of computers and was then the right thing to do—sometimes the only possible thing to do—because the early computers were small and expensive and we needed to save as much space as we could.

Unfortunately, this method of programming became a habit and we just kept on using it. The result is that the problem is now widespread through millions of conventional computers and an unknown number of other types of electronic locations as well, and every one of them is just waiting to start misbehaving, if not now, then when we get to 2000!

Time horizon to failure

Think of a business process in your organisation where you look forward into the future—setting your budgets for the next financial year or making sales forecasts could be examples. Do you know that your system is ready for the Year 2000? If it is not, then you have until you first have to cross that 1999/2000 boundary *in any process* to put things right. That is your Time Horizon to Failure: the time within which you need to correct the problem. Within that time you probably need to fit some sort of a time buffer as a safety margin as well.

Think about the Time Horizons to Failure for your business processes. Remember that many organisations have been hit by the Year 2000 problem already. How long do you think you can safely delay checking to find out if you have a Year 2000 problem?

It's unlikely that you can afford to delay at all in assessing your exposure. Until you know the extent of your risk, you are flying blind in the certain knowledge that there are dangers out there.

So, why all the fuss?

This is a fair question. Surely this sounds like just the kind of problem that computer people and computers should be very good at solving. To some extent that's true. But the reason the total problem is so difficult is because of its scale, variety and complexity. Worldwide, there could be around 10 billion uses of two-digit dates in computer programs. Each of these has to be identified and corrected, or the programs themselves have to be replaced. Either option comprises an enormous workload. The programs are written in many different languages and dialects of languages, and each requires its own set of skills and techniques. Computer people and the automated tools they use tend to be specialised. To add to the problem, many business processes are performed through different programs, people and equipment all working together. Having fixed all the individual bits, you have to ensure that they all still work together properly.

This may be the sort of challenge relished by computer people, but not necessarily by the business people who are also going to be involved. And the trouble is that we are starting maybe two to four years too late for all the work that lies ahead to be done in time. We should be at least halfway through, whereas we are really only just starting. Hence the urgency; hence the fuss. There is too much to do and too little time!

ACTION POINTS

1. List the critical business processes for your organisation—the ones that must not fail if you are to stay in business.
2. Do you know (not just think you know, but really know) the extent of your organisation's risk from the Year 2000 problem?
3. What are the processes in your organisation in which you could have Year 2000 problems before 1 January 2000 if they are not Year 2000 ready?

NOTES

1 The diagnosis was apparently assisted by a telephone call from Tasmania to New Zealand which revealed that, because of the two-hour time difference, the problem had struck the Australian plant two hours after the New Zealand one. It had to be something to do with midnight *local* time.

CHAPTER 2

How it happened

It seemed (and was) a good idea at the time...

It all started as a very good thing to do. Thirty or so years ago computers had very small, very expensive stores in which to keep the programs and the information, such as dates, with which they worked. The pioneers who wrote the early programs of computer codes needed to save every possible storage location in the computer. Leaving the '19' off the year in any date that was involved was one easy way to do this; you wrote the program to assume that '65' in a date, for example, actually meant '1965' every time.

I can remember writing code that did precisely this in 1965 when I worked in the computer operation of a freezing company. To check the 'sanity' of any date entered into the computer, we had to check to see that the year was greater than 64. We programmers knew this wouldn't work when we got to 2000 because the computer would reject a year of 00, but we were certain that those programs wouldn't be around then and neither, probably, would we!

Ten years later we had become very proficient at handling two-digit years, so why reinvent the wheel? It was still good for 25 years yet—several lifetimes in a computer sense! And we were still trying to come to grips with how to use and manage this technology.

Ten years further on again, in the mid-1980s, we were deluged with all manner of riches in the form of immense computer power, enormous storage capacity, the ability to communicate data electronically and our own personal computers. There was no longer any need to save a couple of digits from the year: we now had millions of storage locations available, not just a few thousand.

But in the information technology industry we had many really big challenges to overcome—and computer people revel in challenges! As needs grew, we often didn't bother to redevelop existing systems; we just transferred them to run on newer, more powerful equipment. We concentrated our creative attention on the entirely new types of systems that were becoming feasible. The result was that in most situations we just carried on using the old methods to handle dates. We just never thought about it, because this was one of the areas where we felt confident that we knew what we were doing. In the meantime, we had plenty of other much more pressing things to worry about.

So most of us never had occasion to stop and question the long-term viability of this programming habit we had got into. If we had stopped, we would probably have said that no one in their right mind would still be using these programs in 15 years. Just look at how rapidly technology was advancing! By this time, a small number of computer companies were producing computer systems based on new and different designs, and some of these—for example, Apple Macintosh—used the full four-digit year as a matter of course. These systems will probably avoid the Year 2000 problem. But microcomputers embedded in silicon chips were coming into use then as well. Some of these had storage limitations. Some of them were associated with internal electronic clocks and these tended to use two-digit years.

Now in the 1990s we are waking up to the problem, programmers and business people alike, but rather too late.

Other factors haven't helped

A number of other factors have contributed to the perpetuation of this 'blind spot'.

A lack of professional responsibility

People working with computers have, too often, failed to recognise that what they do is essentially just another form of engineering. Engineers in any field are trained to acknowledge the importance of any limitations in the things they design and produce, such as use-by dates. They understand their responsibility to notify any such limitations to clients and users. Yet prior to the eruption of the Year 2000 problem as a global issue, I don't recall any instance of a Year 2000 use-by date being volunteered by the supplier of a piece of hardware or software. Nor, until very recently, did customers ever consider specifying Year 2000 readiness for a system.

Unfortunately, the engineering profession has been slow to welcome people who engineer with computers into their ranks. And in those few countries, such as the United Kingdom, where they are able to be so accepted, only a small minority of computer practitioners choose to do so. People in the information technology industry have tended to shy away from adopting codes of good practice and accepting imposed standards of professionalism. They are able to claim, with some justification, that many of the extraordinary successes of their industry are the result of creativity in the face of constant change and that creativity flourishes best when unconstrained. They seem to have difficulty in accepting that discipline is not inevitably the enemy of enthusiasm. In any event, discipline of any kind is very hard to impose where you are dealing with the free market at its most successful and innovative and you are dependent on the specialised skills of a limited pool of people. It is true that computer and information skills have for some years been taught in this country as 'information engineering' and 'systems engineering' and that these labels do imply the sorts of intellectual disciplines that engineers use, but the sense of responsibility for the ongoing integrity of the final product isn't there yet. If it were, we would not be trying to come to grips with such a massive problem so late in the day.

The microchip explosion

In the last decade or so, computer programming as an activity has expanded from its conventional areas into the programming of microchips, massproduced and embedded in otherwise ordinary equipment of all kinds. It has taken with it many established techniques, such as two-digit dates. The problem thus extends now beyond computers and into the realm of mobile phones, lighting systems, vehicles, white goods, plant, and so on.

The 'DP personality'

People who work with computers in conventional data processing (DP) have been shown as a group to fit a certain type of personality profile. One characteristic of this is a higher need than individuals in any other professional grouping to feel that they are growing personally in their work. They need to feel constantly challenged. There could be little challenge for them in redesigning boring old date routines!

Top managers have been slack

The final factor has been neglect by the managers and owners of our organisations. Perhaps because they have been baffled by the jargon and burned by early disappointments, many senior managers have abdicated their responsibility to apply their normal standards of scrutiny to the management of anything to do with computers. Unrealistic demands, lack of understanding and neglect are frequently cited by computer people to describe the way the businesses manage them.

In turn, business people often criticise computer people for a failure to understand the needs of the business and a general unwillingness to 'fit in'. The focus of the business has been on immediate delivery of benefits to the business at minimum cost. There is nothing wrong with that, but it has been at the expense of such considerations as the quality of the offering and its anticipated lifetime.

Raising the alarm

In 1991 a Canadian named Peter de Jager first began to draw public attention to the potential scale of the Year 2000 problem through an article in a major computing journal. He was especially concerned at the extent of the occurrence of two-digit years in the massive computer programs, now called legacy systems, used by the huge and complex organisations in the United States. These systems typically run on large computers called mainframes, from IBM or its rivals, and have been built on repeatedly over many years to meet changing requirements.

The systems are most often written in a programming language called Cobol and are riddled with two-digit dates—in fact, so many two-digit dates that de Jager's calculations suggested there might not be enough Cobol programmers in the world to correct all the Year 2000 problems before they hit us, even if they worked on nothing else. One thing was certain: these programs would malfunction at 1 January 2000, if not before, and their organisations would suffer a disaster, and probably go out of business, if nothing were done.

Initially the response was slow, but more recently the media have picked up on the issue and realised that it is not a beat-up scare story but a real one. De Jager's reasoning has been judged sound by many experienced professionals in the field who have studied the problem carefully. And the range of the problem is now known to be much wider than just the old legacy systems on massive mainframes. It may affect personal computers and the programs running on them, the software packages running on the medium-sized computers that many Australian businesses depend on, electronic chips embedded in equipment such as vehicles and security systems, and infrastructures such as telephone exchanges and switches. Unfortunately, 1 January 2000 is not the only date when aspects of the problem could strike. Bear these possibilities in mind:

- *1 January 1999 and 9 September 1999:* Many systems have used '1/1/99' and '9/9/99'—or simply '99'—to signify 'no expiry date'. 1 January 1999 is also likely to be prone to the unexpected because on that day many forecasting and budgetary systems will look forward for the first time into the Year 2000. On 9 September 1999 many computer files on magnetic tapes marked with that date to ensure they should be kept forever will suddenly become free to be overwritten with new material.
- *31 December 1999:* '31/12/99' is commonly used as a 'die date' and will cause some systems to stop altogether. (An interesting side issue is that 1 January 2001 is where the 21st century actually starts, so 1 January 2000 marks the move to the next millennium but not to the next century!)

- *29 February 2000:* The Year 2000 is a leap year.
- *31 December 2000:* This is the 366th day of the year. Some systems will be expecting only 365 days (just like Comalco's aluminium smelters in Tasmania and New Zealand on 31 December 1996!).

The bad news and the good news

There are two especially worrying aspects to this business:

1 We have at most from now until the end of 1999 to diagnose, fix and test that we have properly remedied our problems and not introduced new ones.
2 In some types of situation, particularly that of embedded chips, we have no real understanding of the extent of the problem or how to deal with it with certainty.

The upside is that there are some very good people working in the Year 2000 field who have thought their way across the full range of the problem. There is broad agreement as to the approach to take. It is the same approach you would take to deal with any major threat of unknown size. It is called risk management. It's not rocket science; it is really more like applied common sense.

This book will help you to apply this common-sense management to your risk from the Year 2000 problem so that you can handle it in the best way possible. You may find that you have no real problem at all—in which case you should look to your opportunities because you can be sure that not everyone in your business or industry will be as well placed.

ACTION POINT

If you knew that your organisation was going to be ready for Year 2000 in time and that some of your competitors were not going to be, how could you turn that situation to your advantage?

3 CHAPTER

How you may be affected

In Chapter 2 we saw how the problem arose and how it has crept up on us stealthily so that we are all potentially threatened by it. In this chapter we outline the breadth of the problem—the variety of areas within a business or organisation that could be affected. This will allow you to make a preliminary assessment of where you may be hit. In the following chapters we will look at each of these areas in turn.

Conventional computer systems

Many types of business functions are now performed on conventional computer equipment installed in computer rooms in your own organisation or supported by other organisations for you. For example, you may run your accounts on your own computer or your accountant may do this for you.

Conventional computer systems are used for such purposes as financial accounting, stock management, distribution, purchasing, and so on. They may serve localised parts of the business or support activities that are distributed through computer terminals of different kinds. Often they house vast quantities of your organisation's information. The problem may be contained either in the information or in the computer systems themselves. Chapter 5 will explain how to assess your exposure.

Personal computers

Your personal computers may be susceptible to the Year 2000 problem in various ways or not at all. One of the factors is their age, but you would be wise to check in all cases.

We invest in personal computers in order to run software products on them to do things like word processing, forward planning, surfing the Internet, playing computer games, and so on. These products have names like Word, Excel, Lotus 1-2-3 and Netscape. Some of these, particularly in their earlier versions, may contain the problem. This means some of the work we do using them may be affected.

Chapter 6 discusses in more detail how the problem affects personal computers and the ways in which we use them.

Plant and equipment containing embedded chips

This area is felt by many experts to be potentially the most troublesome part of the whole problem. To get a feel for the scale of the potential difficulties, consider this: in 1996 over two billion electronic chips embedded in equipment of various kinds were shipped globally. Compare that number with the mere 50 million Pentium chips delivered in PCs during the same period!

The problem is that no one has a handle on the Year 2000 status of those embedded chips. We know that some will contain internal clocks and use two-digit years, while others will have no involvement with any kind of timing. The trouble is that so far we have no simple way of finding out which is which.

So, you probably have some of these embedded chips, and you don't know—and I don't know—whether they will still function in 2000. Is all lost? No! But this is an obvious area of risk that you need to manage your way through, so read on. Specifically, read Chapter 7.

Data networks and linkages

Modern businesses frequently operate by transmitting information in electronic form across networks within buildings, between buildings and sites, and between different organisations in widely dispersed locations. Jargon names like LAN (local area network), WAN (wide area network), EDI (electronic data interchange), intranet, Internet and World Wide Web are used abundantly (sometimes bafflingly) by technical people to identify these mechanisms.

The point we need to understand is that all of them require electronic intelligence in order to function. This is provided in devices with names like hub, router, switch, exchange and server. Any of these devices may contain a Year 2000 problem.

This is a specialised area and you need to discuss your Year 2000 exposure with the suppliers of your equipment or whoever provides you with support for it. The equipment involved may take the form of 'black box' PCs or of embedded chips, so both Chapters 6 and 7 are relevant.

The other organisations on which you depend or which depend on you

This is a 'food chain' issue! At one end of the chain your organisation probably depends on other organisations, like your suppliers of goods and services, your business partners and your other stakeholders. Will they survive the Year 2000 so that they can still do business with you? If you do damage to them because of your unresolved Year 2000 problems, will they sue and do damage to you in return? And, at the other end of the 'food chain', will your customers be Year 2000 ready and so able to continue to provide you with work and revenue? See Chapter 8 for guidance on your business and technical suppliers and Chapter 9 for information about customers.

Infrastructures

You need to know that your power supply company will continue to supply, that you will still be able to make telephone calls and send faxes, that you will be able to use transport when you need to and that the banking system will still function. Can you be sure that all of these will handle the Year 2000 successfully? Read Chapter 10.

A threat or an opportunity?

Chapter 11 contains a discussion of the national and global implications of the Year 2000 problem and the opportunity it could present for Australia and for you.

ACTION POINT

Cross out any of the following areas if there is no way in which it could contain a Year 2000 risk to your organisation:

- conventional information systems
- personal computers
- applications running on personal computers
- data networks
- embedded chips in equipment
- infrastructures like banks, telecommunications, transport
- your suppliers
- your customers
- your other stakeholders
- your industry

If some of the above areas are not crossed out, then you need to read on. Even if you *have* crossed them all out, you should read on anyway to ensure that you fully understand the nature of this problem.

CHAPTER 4

‘Year 2000 ready’ or ‘compliant’

What do we mean by being ‘ready’ for the Year 2000 or ‘Year 2000 compliant’? There have been numerous attempts to define this concept. We need a description of exactly how every aspect of our business will behave (so that we can be sure that all the numerous *possible* bad things will not happen) as we move from 1999 into 2000 and on to 2001. We have to bear in mind, as an added difficulty, that 2000 is a leap year, though the normal rule would have it not so.[1]

The British Standards Institute has come up with a simple statement of what desirably should apply. The standard, coded for reference purposes and known as DISC PD 2000-1, consists of four rules. If everything in your world follows these four rules, then you will sail through to the next millennium unscathed. This is the objective standard to be achieved by your business and all the other businesses on which it depends.

> **DISC PD 2000-1: A definition of Year 2000 conformity requirements**
> Year 2000 conformity shall mean that neither performance nor functionality is affected by dates prior to, during and after the Year 2000. In particular:

Rule 1: No value for current date will cause any interruption in operation.
Rule 2: Date-based functionality must behave consistently for dates prior to, during and after Year 2000.
Rule 3: In all interfaces and data storage, the century in any date must be specified either explicitly or by unambiguous algorithms or inferencing rules.[2]
Rule 4: Year 2000 must be recognised as a leap year.

This, or a similar, wording should form part of any contract for purchase of goods and services that you sign from here on until well past the start of the next century—that is, until 2001 at least.

NOTES

1 The normal rule is that a year is a leap year if it is exactly divisible by four (such as 1996) unless it is also exactly divisible by 100 (such as 1900). However, if a year is also exactly divisible by 400 (such as 2000), it is a leap year.

2 Don't worry about the technical language in Rule 3. It just means that any date represented in any way should be unique so there cannot be any confusion about which century is being referred to. Any year with four digits will be unique. Any year represented with only two digits will be allocated in a predefined way either to 19XX or 20XX. The years may be split evenly. Thus, 00 to 49 might go to the range 2000 to 2049; 50 to 99 to the range 1950 to 1999.

5 CHAPTER

Conventional computer systems

The comments in this chapter apply equally to your own computer systems and to those of other organisations on which you depend.

The global estimate is that 90 per cent of all systems will be affected by the Year 2000 problem in some way. However, a lot depends on the nature of the business. For example, inventory systems for a pharmaceutical company are much more likely to be concerned with dates of manufacture and expiry, and hence are more potentially liable to the problem, than inventory systems for an automotive parts distributor. There is some anecdotal evidence that, over all, the percentage of systems affected may be lower in Australia than in larger developed countries. But this doesn't mean that you can ignore the problem!

Bear in mind the following points:

- The older your systems are, the more likely they are to contain the problem. But just because they are brand new, or the computer they run on is proudly claimed to be compliant, it doesn't mean that the programs themselves are compliant. Modern computer systems can actually be best viewed as consisting of a series of layers of which the computer hardware is only one. Each of the layers needs to be Year 2000 ready, and they all need to work together in a way that is ready for Year 2000 as well.

- Some systems, amazingly, are still being written today using two-digit years.
- If a program has the problem in one place, it probably has it in lots of places. One test will not tell you all you need to know.
- A business process may involve more than a single program running on a single computer. For the process to be ready for the Year 2000, all parts of it must be ready.

How can you tell if your systems have the problem?

There are a number of ways in which you can find out whether a computer system has the problem.

- Talk to the people who wrote it or installed it or who are responsible for maintaining it, and insist on answers that you can understand. If you have any doubts at all, ask them to show you proof of their claims. Establish whether they are obliged to remedy a Year 2000 problem, if it exists, under your contracts for purchase or maintenance. (See Chapter 12 for an outline of the legal aspects.)
- Have someone who understands computer code and documentation look at these items for your systems. (Sometimes you will not have been provided with these materials by your supplier or developer, or they may have been lost.)
- Test it. This may be more difficult than it sounds, it may be hazardous, or it may not be possible at all. Don't try testing your computer systems without good technical advice and a thorough testing plan to guide you.

What remedies are available?

Lots of tools; no silver bullet

Automated computer tools are becoming available for scanning computer programs for two-digit year codes and even for correcting them. These come in a wide range of forms, from small programs run on a personal computer on your own premises to massive powerful combinations of hardware and software, in factories, to which you send your programs for treatment. The tools often come with a specialist operator. For all that, they can often be cost-effective in comparison with using human programmers alone.

These tools are likely to become applicable to a growing range of situations and to pick up an increasingly high proportion of the total occurrences of the problem as global Year 2000 experience grows. However, it would be very unwise to wait around for a 'silver bullet' that will solve all your problems. This is not the sort of problem where you can afford to hang out for the Lone Ranger to ride into town!

The total task involved in dealing with the Year 2000 for conventional computer systems is a series of steps, starting with identifying what systems you use and the extent to which they suffer from the problem, and then, if you aren't going to go for total replacement, fixing all the problems and testing to ensure that they have been remedied. This testing is required whether you are repairing the old system or installing a replacement.

The new automated tools can assist in various parts of the total task, not just the code scanning and fixing, and are becoming increasingly powerful. But they can carry out at most 20 per cent of the total work required in diagnosing and remedying the problems. Regardless of what tools you use, the largest work effort—50 per cent or more of the total—will be testing to see that the new or repaired systems work correctly in all respects.

Upgrade your way to safety

When you buy software in the form of a package, quite often the supplier provides you with new releases from time to time. These contain corrections to 'bugs' that have been reported, new functions and other improvements. They generally come as a part of the maintenance contract. It many cases it is optional whether you implement new releases or stay with what you have. It is always possible, therefore, that your package is not Year 2000 ready but that there is or will be a later release that is. You could upgrade to it. But you need to check the following:

- Is the upgrade one that carries with it a tag: 'Oh, by the way this upgrade will require that you buy all this extra hardware as well'?
- Will the upgrade be easy or hard for you to achieve? If, to get to safety, you need to move through each of several intermediate releases

to get to the one you need, the total amount of work may just be too great.

System replacement or repair

If a suitable upgrade isn't available, you may have to choose between replacing the system with a new one that is Year 2000 ready and repairing the one you have. Either could be an expensive route. Selecting and implementing a replacement system could also be a lengthy process. With a replacement you will have the benefits of an up-to-date model, but you will also have to undergo all the changes to the way you do things that come with having a new system. By comparison, the repair route will probably be cheaper and quicker, but what you will get is just a Year 2000 ready version of the same old system.

The biggest obstacles

Time is running out

Whatever option you choose, the scarcest resource of all for dealing with the problem is likely to be time.

The crux of the matter is the impact that the problem, if not corrected, could have on your business. If it is a matter of survival, cost may be less important than finding a solution that can be implemented in time. And, unfortunately, you may have less time available than you thought. Remember that it is dangerous to assume that you have until the end of 1999 to fix any problems. The time you have available to fix or evade any Year 2000 problems in a system is the time until it fails in such a way that it cannot be put right through normal maintenance. That is your Time Horizon to Failure for that system. As we have discussed, in some applications—financial systems are an example—the problems, if they exist, will occur much earlier than 1 January 2000. Financial systems, if they are not Year 2000 ready, will strike the problem when the accounts are first set out for the financial year that crosses the 1999/2000 boundary.

In calculating how you will use the time available to solve your problem, you should aim to complete the process, including testing that all is now well, some time before the date the problem is expected to strike, in order to allow a buffer for safety. Three months would probably be an adequate safety margin for most situations.

Shortage of technical expertise

The next most scarce resource could be people with the right set of technical skills. It may well not be easy to find the skills you need either to implement a replacement system or to repair an old one. This difficulty will get worse as time goes on. As the millennium approaches, skilled computer people of all kinds are going to be in shorter and shorter supply, in part because, human nature being what it is, far too many organisations will leave their Year 2000 efforts until far too late.

ACTION POINTS

1 Make a list of the conventional information systems your organisation uses.
2 Do you know the extent of the Year 2000 exposure in those systems?
3 Which systems support the processes that are essential for you to continue in business?

6 CHAPTER

Personal computers

The hardware

Personal computers (PCs) contain an internal electronic clock that has its own battery electric power supply and keeps the computer alive, as it were, when it is not switched on. For most of their history the internal clocks in PCs have recorded the year as two digits. Fully compliant hardware with internal electronic clocks using four-digit years was, in 1997, only starting to be delivered in Microsoft/IBM family PCs.

In fact, most PCs[1] delivered since the beginning of 1996 have in practice been Year 2000 ready. This is because a PC component called the BIOS (basic input/output systems) chip has been designed to take corrective action when their internal clock first comes up with a two-digit year value of 00.

The BIOS chip in older PCs wasn't set up to do this. When the clock in one of these older PCs ticks over at midnight on 31 December 1999, its date will shift from something like 311299 to something like 010100. The effect will be that the computer will appear to have had its date reset to some earlier time—the beginning of time so far as that PC is concerned. And that is the date that programs running on the PC will use instead of 1 January 2000. The results will be unpredictable and almost certainly wrong. When the PC is then used, for example, to produce invoices or letters, they may have dates from the past printed on them. In most cases the non-compliant computer will also have the wrong day of the week in mind. Whereas 1 January 2000 will be a Saturday, 1 January 1900 was a Monday. So, if such a PC were being used to control your building's security system, it may open the doors while you and all your colleagues are at home enjoying the first day of the holiday weekend after seeing the old millennium out and the new one in!

Here is another example of what might happen. Some lift-control systems are set up to work most efficiently when coping with peak traffic loads on weekdays. At weekends they have a rest and accommodate maintenance periods, expecting to have very small traffic loads. All this intelligent behaviour may be provided through a PC. Imagine now that the PC thinks that Saturday is a Monday, as it may in January 2000 if it is not compliant. All will be fine until the first Thursday and Friday, when the lifts will go to sleep for what they think is the weekend, affecting thousands of office workers in high-rise office blocks! It is fortunate that the problem will strike us at the start of a four-day holiday weekend, when most systems will not be under heavy load and, if problems do arise, there will be a little time available for dealing with them. But don't take the attitude of a European information technology manager recently quoted on the Internet to the effect that the long weekend would provide lots of time for fixing any Year 2000 problems so he wasn't going to do anything about it until then!

The good news (for some) is that all Apple Macintosh personal computers are ready for the Year 2000.[2]

Remedies

If you are not an Apple Macintosh user, you need to find out the Year 2000 status of your PCs and your options for any needed remedies. For the bulk of people, whose PCs belong to the Microsoft IBM world, Year 2000 compliance test kits and techniques are available, *but please note—and use—any precautions in the instructions*. Quite simple remedies are available in some situations. Some diagnostic tools are available free over the Internet; others cost up to about $100. Replacement hardware components may be a little more expensive to purchase and install.

The bad news is that, unfortunately, it appears you will need to investigate each PC individually. It has been found that suppliers have used different components, even recycled components, in different batches of the same model.

An alternative strategy could simply be to upgrade to new equipment that is Year 2000 ready. There are undoubted benefits in upgrading your PCs every few years anyway, to take advantage of the immensely powerful features being introduced continuously. So, if the PC you have is not Year 2000 ready, upgrading to a new one that is should be a serious option for you, even if you do feel a bit sore about the computer industry having dumped this problem on you.

The software

It's not just the PC hardware that may not be compliant, but also the operating and office product software you run on it. Current versions are more likely to be compliant. You should consult your supplier about the status of your software and what your options are. Their advice is likely to be to upgrade to a compliant version. With luck, there will be a compliant version already available.

Some suppliers have published some kind of document setting out the Year 2000 status of their products. You should ask to see one of these. For many products the use of two digits will continue to be allowed. For these the document should spell out a 100-year window within which any two-digit year will be assumed to fall by the software. This window may well be sufficient for your purposes.

The supplier is also likely, in any event, to disclaim responsibility for the way in which you have used or will use their software. For example, many versions of PC software permit you to use either two-digit or four-digit date formats for input and output. If you have chosen to use two-digit years, then the consequences are yours to bear, not the software supplier's. This would apply equally to data you key in yourself and anything you download from another system.

The new versions of the mainstream brands of PC software (Lotus, Excel, Access, Word, and so on) are all likely to be compliant well before 2000, particularly if you use four-digit and not two-digit date formats. But applications that you have developed using them may not be compliant. Most spreadsheets, for example, are unlikely to be a problem, but those that project forward across the 2000 boundary may malfunction.

Also at risk are spreadsheets and databases that are regularly used, which carry data forward from one run to the next and are modified from time to time. They have often been written by users who, understandably, have no particular knowledge of good programming standards and techniques. They may end up in a state where no one really understands how they work or even what they do, except that they are vital to the business. And they are extremely likely to be full of Year 2000 problems. The remedy here probably has to be either to replace them or stop using them.

Lots of strange outcomes are possible

People in the Year 2000 business entertain themselves by collecting the dates that PCs may come up with in place of the correct one on 1 January 2000. Dates I have heard mentioned include:

- *Years*: 1900, 1980, 1984, 1994, 1999.
- *Months*: January, March, April, December.
- *Days*: 1, 3, 4, 31.

There can be confusion between, for example, the American and British ways of setting out dates. In Britain, 1 March 1999 is represented as 01/03/1999; in the United States, it is 03/01/1999. When your clock says 010300, there can be uncertainty as to the day and month, never mind the century!

The application programs running on the computer often seem to maintain their own dates rather than referring to the PC's clock all the time. Differences of opinion as to the correct date are very likely after 31 December 1999, depending on whether you look at the PC's date or the application's date on your computer screen.

Hidden PCs

PCs are often used as a 'black box' within an interlinked process—for example, in data networks—and often don't look at all like the normal PC. Quite often these are older models, soldiering on in performing the functions allotted to them and not needing to be replaced by newer models offering increased power and functionality. They are very likely to be a source of Year 2000 problems.

Some practical guidelines

There are several options available to you in diagnosing and managing your Year 2000 problems on personal computers. It may end up costing you some money but, allowing for that, this is one area where the problems are relatively straightforward to deal with. But, in doing so, there are a few points to bear in mind:

- You need to focus first on the applications that are of business significance. Personal support and convenience aspects are of secondary importance.
- Focus particularly on the programs that have been developed by users rather than computer professionals, and which perform functions that are of major importance to the business.
- If you decide now that you will deal with any problems at a later stage, but before the Year 2000 strikes, by replacing what you have with more modern items, don't then forget to do so. A delayed replacement may not be a particularly good option in any event if you are going to require technical support to accomplish it. Remember that technical support is going to become more and more scarce, and therefore more and more expensive, between now and 2000.
- Get written statements of compliance from the supplier for any equipment you purchase from now on.
- Get rid of any non-compliant equipment that you decide to replace. Old PCs have a habit of hanging around in an organisation. Old non-compliant equipment lying around the place is just an accident waiting to happen!
- Be responsible in how you get rid of that equipment. You may not be doing the local high school, for example, a great favour if you pass on some 'free' equipment to them without making it clear that it may have a 'use-by' date.
- Ensure that from now on everyone understands always to use four-digit year options and never two-digit years when developing new programs on a PC. (Make sure they read this book and understand the problem!)

PC programs tend to have a short life; the fewer that are left hanging around on 1 January 2000 in a state which could cause problems, the better. Opinion is that simply introducing good four-digit year practice from now on will reduce the proportion of troublesome programs still being used at 1 January 2000 from around 12 per cent to around 3 per cent of the total number.

ACTION POINTS

1. Make a complete list of your PCs (summarise if you have a lot of them).
2. Do you know when each one was bought new?
3. Do you have a policy of regular replacement for PCs?
4. Will every PC purchased new earlier than 1996 (1997 if it is not a 'name' brand) have been replaced before 2000?
5. Are you running on the latest versions of the software you use?
6. Do you have it in writing from the supplier that your applications software is ready for the Year 2000?
7. Are you confident that if you or your PC users have developed applications to run on them, they have always used four-digit years and never two-digit years?

If you have given any 'no' answers, you could be at risk.

NOTES

1 But not all! Some 'notebook' PCs (the latest small portables) being supplied by normally reputable suppliers in June 1997 were found not to be Year 2000 ready.

2 The Apple Macintosh clock will run out at 6 hours 28 minutes and 15 seconds precisely on 6 February 2040. This should give Mac devotees ample time to sort out what to do then!

7 CHAPTER

Embedded electronic chips

This is perhaps the area of risk that has received the least attention so far. Yet, a number of commentators are saying that this may be the most troublesome area of all: the part of the iceberg that is hidden under the water. At this stage we have no firm grip on the extent of the problem. Very early experience is suggesting that the frequency of Year 2000 problems in embedded chips is around two or three per thousand. This is a much lower level of incidence than is the case with conventional computer systems and PCs. But it is still a significant level because just one failure in the wrong place could cause you endless trouble—so the search for all embedded chips needs to be thorough.

It does appear, though, that you can safely expect to find no Year 2000 problem in most of the chips you find. This may reflect the fact that they tend to be rather simple devices developed to deal with relatively uncomplicated tasks.[1]

If you do find only a very few occurrences of the problem, this is good news, of course, because the cost of remedying your Year 2000 exposure will be much less than it might have been. But the cost could still be significant because it may be that the chip cannot be fixed or replaced and so you have to replace the whole unit in which it is embedded.

Buildings:
- Air conditioning and heating controls
- Access controls
- Fire systems
- Irrigation systems
- Lifts
- Lighting systems
- Automatic doors
- Surveillance systems

Communications:
- Modems
- Routers and Hubs
- Satellites
- Servers
- Television equipment
- Switches

Bank and retail:
- ATMs
- Bar code readers
- Cash registers
- EFTPOS
- Point of sale devices

Plant:
- Energy meters
- Freezer management systems
- Furnace management
- Petrol station fuel pumps
- Plant control systems
- PLCs
- Environment monitoring systems
- Water coolers and heaters
- Weighing machines

Office equipment:
- Mobile phones
- Faxes
- Mobile radios
- Pagers
- PABX
- Phone management systems
- Phones
- Photocopiers
- Projectors
- Time clocks and swipe cards
- Voice mail

Other:
- Aircraft
- Audio equipment
- Automatic monitoring equipment
- Battery charging systems
- Cameras
- Clocks
- Cranes and other lifting equipment
- Credit cards
- Cryptography
- Defence equipment
- Digital cameras
- Digital organisers
- Field data recorders
- Global positioning systems (GPS)
- Hospital equipment
- Kitchen equipment
- Microwaves
- Safes and vaults
- Scientific calculators and equipment
- Speed cameras
- Televisions
- Traffic lights
- Vehicles
- Video cameras and equipment
- Weigh stations
- White goods

The first task is to identify where we might find electronic circuitry; we then need to establish whether or not it contains the Year 2000 problem. Look at the list opposite for a start. Any of these items could contain embedded electronic chips and therefore could be susceptible to the Year 2000 problem. You will almost certainly be able to think of other possible locations.

Just because your use of the equipment doesn't involve dates or even time doesn't mean you are safe. There could be a system clock and two-digit date code in there that is not apparent in use and won't be—until it malfunctions.

If your premises are leased, don't forget the services provided for you by your landlord. You need to know your risks and that your landlord knows to handle them for you.

Where can you look for help?

In general, you cannot look for help from computer people who work with conventional computer systems; this is not their particular area of expertise. This is, or should be, the territory of the engineering profession. It has to be said that engineering bodies have been extremely slow to accept that a problem exists, and Year 2000 articles have only started to appear in their professional publications in the last year.[2] So, to a large extent, at this stage it is a matter of finding help where you can; looking for individuals who are alive to the problem. Word is undoubtedly spreading, though nowhere near fast enough. So you should:

- Look to those people in your organisation, and it might be you, who are responsible for the equipment, especially if they were involved in acquiring it.
- Look to whoever manufactured, supplied or maintains the equipment.
- Consult manuals and other documentation, if you can find them.
- Have a look at the equipment yourself, or have someone technical do it for you. (Beware: this is territory only for the technically well informed or the very desperate.)
- Check if there is a digital read-out anywhere for maintenance or other purposes.
- Check whether the electronic equipment has its own battery power

supply. If it does, perhaps the battery is there to keep an electronic clock ticking over as well as retaining any system settings.

- Consult the manual (if there is one) to see if it throws any light on the existence of a clock.
- If there is a clock, check if it's possible to reset the time so that you can test whether the equipment will successfully roll over to the next millennium or can be started up as though it were actually in the Year 2000.

A warning: before you try any kind of test, check your maintenance and purchase contracts. Don't try anything that could remove any onus on suppliers or developers to fix the problem for you. And don't try any tests without being sure that you can reset the equipment back to the present time and not do any damage as a result of the test.

The great unknown

It is at this level that the situation gives rise to concern. As a Year 2000 colleague, Philip Davies, stated recently: 'Here we are being asked, with two and a half years to go, about the Year 2000 status of lifts and the really scary thing is that we don't know the answer.'

We know that lifts won't suddenly free-fall down their shafts on 1 January 2000, above all because they have reliable mechanical safety devices to stop that ever happening. But for example, they very well might mistakenly decide that now is the time to prepare themselves for maintenance, lower themselves to the bottom and stay there.

It is important to complete a full inventory of any equipment that could conceivably contain the problem, and then to investigate the Year 2000 readiness of each item, using the skills and knowledge of your own staff and of the equipment suppliers and manufacturers. Obtaining sound information about Year 2000 status may take time because this is new territory for suppliers and manufacturers and they sometimes need some persuasion.

You should understand, also, that even the manufacturer of the equipment may not know its Year 2000 readiness and may have to go back to the supplier of the actual electronic components used. The manufacturer may have the added difficulty of having used different electronic chip suppliers at different times for the same model. And, of course, the manufacturer may not still be in business anyway.

Desperate remedies

This type of investigation can take a lot of time and still lead nowhere. So you may be forced to make a decision on the basis that the equipment cannot be shown to be ready, rather than that you know it is not ready. If you cannot find out the Year 2000 status of mission-critical equipment within the time you have available, you may have to consider replacing it, or at least the suspect portions of it, just to be on the safe side.

If it is impossible even to think about replacing all such affected items, work out which ones are mission critical. How many could you live without at a pinch?

ACTION POINTS

1. **Using the table of potential locations for embedded chips as a guide, draw up a list for your organisation. Then, for each item, think about the impact on your business if it failed at or before 1 January 2000.**
2. **Which items couldn't you live without?**
3. **How long would it take to replace each of the essential items, if you had to, because it was incurably afflicted by the Year 2000 problem?**
4. **If your premises are leased, is Year 2000 readiness for the lifts, security, environmental controls, roller doors, fire safety, irrigation and other equipment included in the contract?**
5. **Would it be possible to test any equipment that you feel may have the problem as part of the next regular maintenance cycle?**

NOTES

1 Perhaps they were programmed by methodical engineers rather than highly creative information technology types!

2 The UK Institute of Electrical Engineers has a very useful Web page that deals with embedded chips (see Chapter 16).

8 CHAPTER

Your business and technical suppliers

In an ideal world you would like to know that every one of your business suppliers, including the suppliers of computers, software and other equipment, will be 100 per cent ready for Year 2000 so that they can continue to supply you and support you in a seamless fashion right through into the next millennium.

The practical risk you have to face is that even if you make yourself 100 per cent ready, some of your suppliers will fail to do so. You could then fail because they can no longer supply you with what you need. It would therefore be prudent to find out your main suppliers' Year 2000 plans. It's quite likely, at this stage, that some of them won't know what you are talking about. Or they may still be in the state of denial that seems to afflict us all when we first encounter the preposterous but unfortunately very real suggestion that our computers may suddenly fail because of a silly little technical problem that has been replicated or mutated billions of times. So a bit of missionary work on your part may be needed.

Put the hard word on

Of course, if your suppliers can't or won't acknowledge the problem or fail to convince you that they will cope with it in time, then you will need to make contingency plans for other sources of supply. It will do no harm to make it clear, in a friendly way at the outset, that you are taking this issue very seriously and are prepared to find a new supplier if you have to, though you would rather not have to.

A compounding factor in terms of your computer and equipment suppliers is that they may no longer be in business and so be unable to help you assess your risk from their equipment, or they may elect to go out of business before 2000.

You may have to resort to 'drop dead dates' (more politely known as 'contingency action dates'): 'If I don't have a credible assurance that your equipment or service is Year 2000 ready by the first of next month, I shall assume that it is not and will make plans accordingly.' This may seem tough, but this is a situation calling for tough measures.

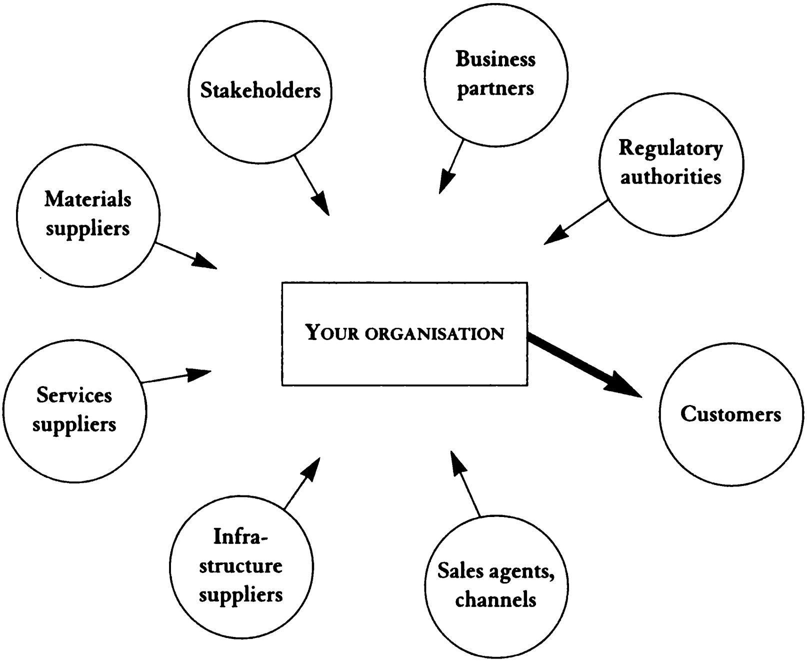
Identify priority areas

Some of your suppliers will be much more important to you than others. The diagram on the next page illustrates a way of thinking that can help you to identify those suppliers who are most important and who could hurt you the most if they were to fail.

Referring to the diagram on the next page, make lists of your main suppliers, business partners, regulatory authorities, sales agents and channels. Then ask yourself: which of these create the most value for my customers? Those are the ones that would cause you the most grief if they failed to survive the challenge of the Year 2000. Those are the ones you should concentrate on. You may even offer to help them sort out the problem.

Help them to help you

It isn't necessarily the largest or apparently most technically aware organisations that are the most important suppliers to you. For instance, you may be very dependent on a small design shop and also be aware that they aren't particularly skilful in handling their technology. In such a case



it will be in your and their interests for you at least to try to encourage them to think about the Year 2000. If you do offer help or advice of any kind, it is important to understand the responsibilities you may be taking on and to understand, and perhaps limit, your legal liability. Adopt a policy of 'All care, no responsibility'.

In any event, it is important to understand your legal situation with respect to Year 2000 issues under your existing contracts with your suppliers and to consult a lawyer if you are in any doubt. Chapter 12 discusses these legal aspects in more detail.

You need to find out your suppliers' Year 2000 plans and monitor their progress so that you can formulate and implement alternative arrangements if you have to. One way to encourage suppliers to share their Year 2000 plans with you is to share your Year 2000 plans with them. After all, they need to know that you are determined to stay in business.

ACTION POINTS

1. In terms of your business survival, who are your critical suppliers?
2. Could you find alternatives to those suppliers if you had to?
3. If yes, how long would that process take?
4. Think about those critical suppliers: are there things that you could do to help ensure that they are Year 2000 ready?

9 CHAPTER

Your customers: Your risk from them and their risk from you

You need to know that your customers will still be in existence and able to purchase from you in the next millennium. In practice, you need to assume that some will not. This is rather a touchy topic, for obvious reasons, but most of the authorities in the field are unequivocal that there will be business failures.

You need also to know that, from a technical point of view, your customers can still do business with you. If a customer's purchasing or payments system has broken down, the impact may be worst felt by you. So you need to have a strategy for assessing your customers' Year 2000 plans. And this should focus most, as with your suppliers, on those customers that are most important to you in a business sense. You need to monitor their Year 2000 progress and be prepared not only to make contingency plans but also to put them into effect if you feel that an important customer isn't going to make it.

Be proactive

As with suppliers, here also there is scope for being proactive and helping out, if only by telling your customers what you are doing for yourself, in order to raise their awareness of the problem. You need to understand very clearly your legal situation with respect to your customers in terms of Year 2000. If you supply anything with embedded chips or software, you need to be particularly careful. The same applies if you supply technical advice and services to the customer because you may, in doing so, be taking on some responsibility for the customer's Year 2000 situation, even if you didn't realise it at the time. Chapter 12 spells out the dangers here.

For your *own* survival, it is important that your customers survive. There has never been a problem quite like this one and you don't have time to address it at your leisure. So, discussing it with your customers is likely to be important both for you and for them. It is certainly not going to be an admission of weakness to acknowledge that you have a problem and to spell out what you plan to do about it.

Lead by example

That is certainly the admirable line that some leading organisations have taken. Telstra has been entirely up-front in admitting that it is treating Year 2000 as a major issue, and the OGIT has recently sent out a Year 2000 guideline brochure to its customers. Overseas, the Royal Bank of Scotland, Marks and Spencer, Telecom New Zealand, British Telecom and Prudential Insurance have also been open about what they are doing to solve the problem. It is regrettable that a number of other leading organisations have been unwilling to come clean about the problem and what they are doing about it. A few are behaving like ducks sailing serenely on the surface of the pond while under the water they are paddling furiously to solve their problems. Unfortunately, a number of others are still thinking no more deeply on this issue than a duck would do. They still seem to prefer to believe, without ever advancing any evidence for the claim, that the whole Year 2000 issue is greatly exaggerated: an exercise in hype by unscrupulous consultants and excitable computer industry spokespeople. In doing so, they are not showing much sense of responsibility or leadership, nor are they assessing their own risk adequately.

ACTION POINTS

1. What would be the impact on your business if 1 per cent or 5 per cent or 20 per cent of your typical customers failed at around the same time?
2. How many of your customers, do you think, are even aware of the Year 2000 problem?
3. How many, do you think, are doing something about it?
4. Does this particularly matter to you? Are you in the happy position that your customers are extremely unlikely to be affected by Year 2000 or, if some of them fail, you will be able to find others?
5. If it does matter to you, are there things you could do to encourage them to address the issue in time?

10 CHAPTER

Infrastructures and your industry

To continue to do business, you need to be sure that your bank will still be operating, that the air and other transport systems will still be able to move goods and people around, that telephones and faxes will still work, that the power and water will be on and that the sewage won't just back up. And that is just for starters. All of these infrastructures depend on control systems that could well be electronic and therefore candidates for Year 2000 problems. Many of them are also vitally dependent on the capture, storage, processing and transmission of vast quantities of electronic information.

Who is doing what?

We know that banks in Australia are individually and collectively working to address their Year 2000 exposure even though they aren't all publicly forthcoming about the matter. The major communications carriers (including Telstra and Optus) have indicated that they are already investing heavily in Year 2000 projects. Government departments are marshalled under the guidance provided by the OGIT. State and territory agencies are also making headway in addressing the problem, and many of the larger public organisations with a major information technology component have their own corporate or company plans.

Because Australia is a relatively small country, its infrastructures may present a set of Year 2000 problems that are relatively manageable in comparison with those of larger developed countries. For example, one might reasonably assume that Australia will be able to continue to operate with an intact banking system from 1 January 2000. We have a small number of banks and very effective clearing systems.

However, working together, the banks constitute the system through which all our money flows and we do depend on their getting it right. It is to be hoped that those responsible for our infrastructures will keep us in the picture as their Year 2000 projects unfold. It is also incumbent on us as individuals and organisations to keep ourselves aware of what is going on and to make contingency plans well ahead of time if we feel we need to.

While we can be cautiously optimistic that these major infrastructures in Australia will hold together, it is much less likely that in detail every aspect will operate perfectly. And one of those details might be essential for you. Much of this will be beyond your control, but you can at least assess your linkages to the infrastructures and check that they are going to be okay. This means you need to know that your in-house telephone exchange, your on-line banking system, your payroll (particularly your payroll!), and so on are all going to work for you in January 2000. Or if they are not, you will need to have thought through well in advance what you will do about it.

The benefits of collaboration

Most organisations are just one of the players within an industry and often are themselves part of an infrastructure. A bank is an example: on the one hand it is a competitor of all other banks; on the other, it is part of a system on which we all depend.

Time is so short and so much needs to be done, even though, we don't have enormous legacy systems in Australia to contend with as they do in the United States. Collaboration within an industry in the face of this common enemy would be highly beneficial. The banks are a good example of collaboration: they have a joint Year 2000 committee for sorting out some aspects of the problem they share. Seminars and workshops on handling the

Year 2000 have also been held for senior managers of government departments and local bodies.

A number of the organisations providing Year 2000 advice and services in Australia are members of the OGIT Year 2000 Committee. The committee was set up by the federal government specifically to raise awareness of this issue nationally. But we need more industry-based Year 2000 groups. There isn't time for individuals to sort out our own Year 2000 problems alone.

So, think about it. Is Year 2000 likely to result in changed business strategies for your industry or for your organisation as one of the players in it? Is there something you ought to be doing to raise awareness in your industry? Or do you see a greater overall competitive advantage for you in leaving them to it?

ACTION POINTS

1 Make a list of your critical infrastructure suppliers.
2 Is your industry:
   - Dependent on dates and large amounts of information (eg banking)?
   - Highly networked (eg telecommunications or fast-moving consumer goods)?
   - Dependent on applications written by users on personal computers (as in some parts of the finance sector)?
   - Dependent on legacy systems, either your own or a business partner's (eg manufacturing, air transport, insurance)?
   - Dependent on automated process control (eg manufacturing, publishing)?

Any 'yes' answers to the questions about your industry mean that it will be prone to the Year 2000 problem, even if your part of it isn't. (You can also usefully apply the same questions to the case of your own organisation, as one unit in the industry.)

ACTION POINTS

3 On balance, which of these best describes the Year 2000 factor?

	For your industry:	For you:
■ a threat	☐	☐
■ an opportunity	☐	☐
■ a balance of threats and opportunities	☐	☐
■ no real impact either way	☐	☐

4 What is the current level of Year 2000 activity in your industry: Everybody's on to it? Nobody even knows about it? Somewhere in-between?

5 Is Year 2000 being specifically addressed in a constructive way (or at all) in your trade publications, seminars and the like?

6 Are you aware of other players in your industry that are already working to remedy the problem?

7 Do you know or can you find out what they are doing?

CHAPTER 11

The global impact and the effect on Australia

Minor glitch or global disaster?

Writers on Year 2000 seem to be shying away from any firm predictions on its wider implications. They tend to repeat the, by now, fairly familiar litany of the hundreds of millions of dollars required to fix the problems globally, the fact that there aren't going to be enough resources or time to remedy all the problems, that there will be business failures and that lawyers will have a field day in the first part of the next century.

Almost no one has taken the argument a step further and tried to answer, in a reasoned way, the question: what are we really looking at here—a global disaster? Some minor inconvenience? Something in-between?[1]

The cost, resource and time projections are developed from known data about the amount of computer code in use and the rate at which people can modify it. In the absence of evidence to the contrary, it makes no sense to assume that these projections are wrong, even though we don't like the implications. So, let us assume that many organisations may face very large and expensive Year 2000 challenges.

A notable feature of information technology projects up to now has been our inability to complete them on time, to specification and within budget.

Given the size of the challenge and the track record, it is most likely that some organisations around the world will fail to respond in time. They will lose the use of their information systems or their equipment.

If similar damage had resulted from a fire or flood, we would call it a disaster. We know from experience of these other types of disasters that organisations which lose their computer systems for longer than about four days, are likely to go out of business; if not immediately, then during the next year or so.

We also know that this is one type of disaster for which organisations will not be able to claim under their existing disaster insurance policies. The insurance industry in the United States has had independent surveys carried out and ascertained that Year 2000 is now a known problem and that there is, in their view, time to fix it. So, no insurance cover. It is understood that some insurance companies are considering offering policies to cover your residual Year 2000 risk if you can demonstrate that you have carried out an approved program of assessing and managing your risk.

The way forward

Simplify to survive

Arguing from the more positive end, we know also, in the words of Bruce Hall of the Gartner Group, (the firm most frequently quoted on this whole issue) that 'people and organisations are extraordinarily capable'. One way in which this will be demonstrated is that smart organisations will not seek to repair all their millions or hundreds of thousands of lines of computer code. Faced with the need to survive, they will simplify the problem by concentrating on the core elements of their business and also by narrowing down considerably the range of ways in which they approach the market and conduct themselves.

As an example, a typical large airline has hundreds of pricing structures with which it competes in its markets. If the systems that run that activity are a Year 2000 disaster area, very likely they could be replaced with a quick and dirty interim solution and maybe just two levels of price: one for those up the front and another for the rest of us down the back! The airline may not be a vigorous competitor for a while, but it will have a much better chance of surviving. (There won't be much vigorous competition for a while from *anybody* until this problem has been worked out of the industry.) In similar fashion, banks and telecommunications companies, if necessary, may seek survival through simplification.

Merge or divest

Others may adopt the track of mergers or divesting themselves of the threatened parts of the business, though this may not be as attractive as it sounds. Merging organisations and their information systems is difficult at the best of times. Where one of the parties has systems that must be replaced by the other's to a fixed timetable, the problem might just be too big. And who would want to buy, at this time, a bank, for example, if they realised its information systems were riddled with Year 2000 problems?

Pull the plug

Others may simply decide to go out of business. Anecdotal evidence suggests that a few organisations are already thinking about it, and they are not fly-by-night suppliers of dodgy computer equipment, either.

Smile smugly

Yet others will rejoice and prosper because, through either luck or good judgment, they have few or no Year 2000 exposures and can sail serenely on.

We just don't know ...

The fact is that no one really knows what is going to happen. There is little doubt that this is a very major issue quite easily placed alongside any of the other technology-related 'own-goals' that humankind has scored against itself.

The likely future for...

... Banks

On a national scale, in Australia, it is reasonable to assume that banks and the banking system will survive, perhaps with some interruption and narrowing of services. But it defies all reason to expect that every one of the thousands of banks in the United States will sail through unscathed. Some banks will end up not sure of who owes what to whom and, particularly, when. As nodes in a financial system, these banks must then gum up the flow of money through them and in and out of the system as a whole. The key question is: how many of these failures do we need before the wider economy starts to be affected?

. . . Airlines

Planes are unlikely to drop out of the sky or become irretrievably lost. Boeing, for example, is understood to have budgeted some hundreds of millions of dollars to ensure that the planes themselves are okay. And planes use several types of navigation systems, not just global positioning systems (GPS), about which it is known that some receivers are likely to fail on 21 August 1999 unless they are modified. The major passenger reservation systems are believed to be Year 2000 ready. But air transport depends on numerous digital electronic systems in less spectacular but important roles—for example, in ensuring that passengers, fuel, meals, flight plans and properly qualified crews are all in the right place at the right time. This may well all happen at the major airports on the major routes, but what about the less frequently used and remote destinations?

It is going to be extremely difficult for airlines to fly their schedules reliably, and for this reason persistent rumours state that some at least do not intend to fly at all on 1 January 2000. It is not clear why 2 January 2000 should be much better, or indeed many days after that.

. . . Telecommunications

Countries around the world interconnect in a global network of telecommunications. The exchanges and switches that enable people in different locations to talk to one another span a full spectrum of technology from manual to the latest digital technologies. These all have to work, first, so that the call can take place and, second, so that the correct person can be billed for the right amount.

As with banking and air transport, it seems most likely that the major channels of communication will still be able to operate but that individual nodes on the network will be suspect or not function at all. It was noteworthy that a spokesperson for British Telecom interviewed on the BBC World Service in June 1997 was not prepared to give any assurances with regard to customers being able to make calls successfully on 1 January 2000 and thereafter. And British Telecom has estimated the cost of its Year 2000 program at £350 million—around A$700 million!

. . . Other infrastructures

The position here is even less clear. There have to be major concerns about both Year 2000 vulnerability and capacity to manage it in areas such as defence, health-care administration and delivery, and the flows of information between the various units and levels of government within a country and between countries.

Australia's incentive and opportunity

This all adds up to some global dislocation. Whatever the extent of the dislocation, *Australia has an incentive and an opportunity* to cope with it better than the larger developed countries.

There is an obvious incentive for Australia to be a developed modern country that is, by and large, ready for Year 2000 in a world where many of the larger developed modern countries are not going to be ready. There must be advantages for exporters who can still supply, backed by a national financial system and transport and communications infrastructures that are still working and a machinery of government that has not become paralysed because the information has stopped flowing.

The opportunity is there because the problem should be less difficult to address in Australia than it will be in countries like the United States and Britain. There are two reasons for this. One is that most other developed countries have a far larger information technology infrastructure than ours, so their largest organisations tend to have at least one whole layer of complexity additional to ours. Where we can do a job with one computer, say, they may have to use many computers and somehow keep the whole thing harmonised.

The United States has tended to use numbers of very large mainframe computers with huge legacy systems running on them which, if a start hasn't been made by now, they have no chance of replacing in the time available. This will make the Year 2000 remedial and testing tasks for their top-tier, nationally 'mission-critical' organisations very much larger than Australia's are likely to be. (Having said that, even if we assume that the problem afflicts only one-fifth of Australian organisations as intensely as it afflicts their counterparts in the United States, this could still represent a cost to fix them of the order of $10 billion. The real question of course is: how many billions will it cost if we don't fix them?)

The other reason this situation presents an opportunity is that Australians are early adopters of new technologies. We tend to like to be using the latest and greatest. This means that our systems and equipment tend to be newer than those of other countries, and so a larger proportion of what we have may already be Year 2000 ready. (But remember software that is not Year 2000 ready is still being marketed. You cannot assume that the system or equipment you installed a few months ago will not use two-digit dates just because it is new.)

So we have, potentially, a comparative advantage in Australia. But this advantage only applies if we start now. We are faced with the same deadline as everyone else and we're starting late. One reason for this late start is that the problem has not made it into the Australian general media over the last year in the way it has overseas. Much more delay and we will have lost both our advantage and our opportunity.

It's down to you!

What then, realistically, are the chances of Australia gaining an advantage from the Year 2000 problem? Still quite good, but only if we all become aware of the problem and act on it.

Australia operates through the interrelated efforts of many organisations. Most are quite small; a few are large. None can be assumed to be unaffected by Year 2000. What is needed is for all of them to be able to assess their Year 2000 risk and handle it successfully. At the larger end of the scale we know that central government and some parts of local government, the banks, commercial telecommunications carriers and airlines are working on their own exposures. Perhaps we can have some confidence that the key infrastructures they represent will handle the challenge satisfactorily.

Some (but certainly not all) of the other major corporations are also awake to the problem. But below that, in the scores of thousands of organisations that keep Australia going, there is a massive lack of awareness about the problem and what it might mean. And there are no immediately obvious places where people in smaller organisations can turn for advice, particularly if they lack the knowledge and confidence to deal with the technical issues themselves.

That is the reason for this book: to encourage readers to look at their Year 2000 risk before it is too late to do anything about it. I hope that any reader, having got this far, will understand that this is a matter of risk management rather than a technical problem, and it is something you can handle. The management of your risk so that you ensure your organisation is able to continue to function may involve identifying, scheduling and monitoring the progress of some technical solutions. This may still be a daunting task, but it is one that it is certainly not impossible for anyone to start to get to grips with, no matter how technically illiterate they may feel themselves to be.

ACTION POINTS

1. **Can you see potential advantages for your organisation as a result of Australia (and you) handling Year 2000 well?**
2. **What potential advantages can you see for Australia if organisations like yours handle it well?**

NOTES

1 Edward Yardeni, Chief Economist of Deutsche Morgan Grenfell in the United States, is qualified to assess these matters. He recently revised his probability for a global recession resulting from the Year 2000 crisis from 30 to 40 per cent.

12 CHAPTER

The legal aspects

There is much justifiable anger that this enormous and unnecessary problem has arisen. There is no doubt that, around the world, litigation on an enormous scale will be one result. Those who have been brave enough to make an estimate agree that the total cost of litigation in the United States arising from the Year 2000 problem will be measured in hundreds of billions of dollars. In comparison, Australia is not a highly litigious society, but there will undoubtedly be issues arising here as well that can only be resolved by the courts.

The legal aspects of the Year 2000 problem are significant not just for after the turn of the century, when the impact will be obvious, but right now, in trying to prevent the problems from arising. Much legal and practical difficulty will be avoided if you take sensible steps before the problem affects you. It is important that we all understand at the outset the legal implications of our own potential Year 2000 problems.

These legal considerations fall into four broad areas:

1 determining your exposure to the problem;
2 acting to rectify the problem;
3 preventing new problems; and
4 the personal liabilities of senior management.

Determining your exposure to the problem

All too often, organisations put steps into place to correct the Year 2000 problem without determining who is responsible for this work and who should pay for it. While it is certainly advisable for you to take steps as soon as possible, it may be that some of the expense you are incurring should be being incurred by someone else. One of the first steps should therefore be to determine where this responsibility lies. You may need to retain a lawyer at this stage, but obviously the more legwork you do yourself the more you will keep costs down. It may well be that a lawyer will save you a lot more money in the long run, particularly if they can successfully shift the responsibility (and therefore the cost) for your problem on to someone else.

Product agreements

Each product involved in the running of your business is likely to be covered by an agreement. Given that a Year 2000 problem may occur not only in computer products but in any product with an embedded computer chip, any technology-related agreement you hold is likely to be relevant.

Computer system agreements in particular usually cover the following areas:

- maintenance agreements;
- agreements for outsourcing;
- software licence agreements; and
- hardware supply agreements.

If you have any problems with the system, including any Year 2000 problem, these agreements should be reviewed to determine who needs to sort it out and who should pay.

Here are some examples:

- A computer system may be supported by a maintenance agreement that runs past 1 January 2000. Although this type of agreement is unlikely to contain specific references to a Year 2000 problem, it will contain more general obligations to keep the system running and trouble-free. If you are able to show that correcting the Year 2000 problem falls within these obligations, then the service provider will be obliged to supply (and pay for) these correction services.

- Most supply or licence agreements contain warranties as to how the product will function. Again, these are unlikely to refer specifically to a Year 2000 problem but may guarantee that a product is defect- or bug-free or that it will function in a certain way or to a certain standard. If it can be argued that any Year 2000 problem is a defect or bug and that the result is that the product does not perform to the warranty standard, then this constitutes a breach of warranty.

Customer and industry supplier agreements

No business works in isolation. You may make all the effort in the world to ensure that you are compliant and then encounter major problems at the turn of the century because your business partners are not. Hence, when considering your exposure to the problem, have a look at your legal agreements with your customers and any penalties for failure to perform, either on your side or theirs. Similarly, consideration should be given to what happens should your suppliers fail to deliver to you due to a Year 2000 problem.

Consumer protection law

Consumer protection law also means that certain terms are implied in these types of agreements. Even if the agreements don't contain express provisions to correct a Year 2000 problem, the law may imply such an obligation. Relevant legislation in this respect is likely to be:

- the *Trade Practices Act 1974*; and
- Uniform Sale of Goods legislation throughout the states and territories.

Whether these Acts apply or not will depend on each individual situation. Relevant factors are likely to be:

- *The role of the other party*. The more the supplier is acting in a consultancy role or designing a product specifically to meet your needs, the greater the obligation to point out shortfalls in the product.
- *The time the agreement was entered into*. The Year 2000 problem has now become a lot more well known and it would be increasingly difficult to argue ignorance of the problem.
- *The monetary value of the product in question*. The more the amount paid, the greater the expectation as to the reliability of the product received.

- *Supporting documentation*. It could be argued that phrases such as 'this system will take you into the next century and beyond' contained in sales brochures or training manuals amount to a representation that the system is Year 2000 compliant.

Acting to rectify the problem

Prevention is better than cure

Why do you need to review these agreements now when they are only relevant if and when a Year 2000 problem occurs? The answer is that, as a sensible person, you want to be proactive in preventing any problem. If you believe an agreement states that the obligation to correct a problem lies with the other party, you can approach them in advance to ensure they are going to do something about it.

Even if the agreement contains obligations only in the event that a problem actually occurs, this may be used to persuade the other party to assist in preventing the problem now rather than having to pick up the pieces afterwards.

In addition, if you don't state the basis for a claim against a supplier now, this may affect your right to do so at a later date. Your purchase agreement may specify a time limit within which you must make any claim. Failure to establish a claim now may also be held as a waiver of your right to do so later, or it may be seen as a breach of your insurance cover if you are trying to claim for loss, such as business interruption, at a later date. (You should also find out whether your insurers need to be notified of steps taken in relation to a potential claim in case failure to do so invalidates your cover.)

Approaching your suppliers

One of the first steps may be to approach each supplier of the goods and services used in your business to ask if their product is ready for the Year 2000. Getting your suppliers to sign off, saying that their product is Year 2000 compliant, will be useful when trying to determine if a supplier will stand behind its product. Such a signed document will prove extremely useful in any action against the supplier should the product fail to be compliant. It is important that you understand what is meant by the term 'compliant'. (See also the comments under 'Warranties' later in this chapter.)

Legal obstacles

Correcting a Year 2000 problem is likely to involve altering or even replacing the particular product you are concerned about. With software programs it could involve a programmer trawling through thousands of lines of computer code to find the date fields and then correcting them. This might be done by your skilled service provider or by your own staff. The service provider may need to remove the code to its premises or perhaps overseas to do the work. But all or any of these options may be prohibited by agreements covering the product you are trying to fix. Legal barriers to your correcting a Year 2000 problem could take these forms:

- An agreement may contain confidentiality provisions preventing the disclosure of components of a product to outside parties.
- You may not have access to the basic components of a product to alter it—for example, the source code of a software program.
- Even if you do have access to the basic components, such as the source code, an agreement may prevent the alteration of the code or allow it only with the consent of the supplier or licensor of the product.
- The agreement may prohibit the use of other tools, such as other software, in conjunction with the software program in question.

It is important to read the fine print on your product agreements, or you may find you are in breach of them. The consequences may be termination of these agreements, or you could even be sued for breach. You will almost certainly jeopardise any claim you have against the other party for a Year 2000 problem if you have altered their product without their consent.

ACTION POINTS

(Only provide cursory responses to the action points in this chapter on your first reading of it. In due course you will need a full understanding of your legal situation if you are to be fully protected, and this may involve your taking legal advice.)

1 Make a complete list of the agreements relevant to your business.
2 In any case where you don't have a signed agreement, do you have relevant background correspondence that addresses the legal relationship between the parties?
3 Is any step you intend to take to prevent a Year 2000 problem prohibited under agreements relevant to the product you are working on?
4 Do you require the consent of other parties to alter the product, and what form should this consent take?
5 What could be the consequences of failing to comply with these agreements?

Preventing new problems

Any new agreements being entered into should obviously contain provisions addressing the Year 2000 problem.

Warranties

You should ensure that any warranty for anything you buy between now and the Year 2000 specifies that the product is Year 2000 compliant. Of course, here the question arises of what is meant by the term 'compliant'. The suggested British Standard wording is provided in Chapter 4, but other standard wordings are being developed and your supplier may be committed to one of these. Whichever wording you agree on, you need to be satisfied that it will give you the Year 2000 protection that you need.

Ultimately, the effectiveness of any warranty is a matter of negotiation and depends on the relative bargaining strength of each party. You may be forced to accept a much more restricted warranty than you would like.

Testing methods

Many computer-related agreements contain acceptance testing provisions. This means the product supplied has to meet certain functional criteria agreed between the parties for a certain period. You should ensure that any such criteria cover testing for a Year 2000 problem. One obvious difficulty here is agreeing on a method of testing that will show up a Year 2000 problem in the product without damaging other products running in conjunction with it.

Maintenance agreements

When contracting for the supply of services—for example, negotiating a maintenance agreement—the wording should specifically state that the services cover planning, preventing and correcting any Year 2000 problems. You should also consider whether these services are to be supplied for a fixed fee or on a time/cost basis.

Accessing basic components

As mentioned earlier, one of the major difficulties in fixing a Year 2000 problem in a product can be not having access to its basic components, such as the source code of a software program. It is therefore important that this issue is addressed in any new agreement entered into. It may be that the supplier is happy to supply the source code with the product, or it may be that you can enter into an 'escrow arrangement' whereby a third party will hold the source code and release it to you under certain circumstances, such as the occurrence of a Year 2000 problem.

Negotiating liability

The extent of liability of each party should also be considered. It is common to find limitation or exclusion of liability clauses in these types of agreements. A supplier may limit its liability to $10 000 when in fact the problem is likely to cost you $100 000 to fix. The supplier may also exclude consequential loss, such as loss due to the interruption of your business from a Year 2000 problem.

On the other hand, you may expressly state that you will receive liquidated damages (a specified amount intended to reflect your loss) in the event of a Year 2000 problem. Again, these issues will depend on the bargaining power of each party, but you should try to ensure you have a reasonable margin of loss that may be recovered from the other party should a problem arise.

ACTION POINTS

6 Do all your staff who may enter into purchase or sale agreements on your behalf know that the Year 2000 problem should be addressed?
7 In the cases of both sale and purchase agreements, are there warranties that the product or service is Year 2000 compliant and is the term 'compliant' clearly defined?
8 How is the Year 2000 compliance of the product or service to be tested?
9 Are there legal barriers to your access to the basic components of a product required to correct a Year 2000 problem yourself if need be?
10 List any major barriers.
11 Is the potential liability of the other party adequate to cover any potential loss you may incur due to a Year 2000 problem?
12 List any major inadequacies.

Personal liabilities of senior management

In the case of businesses run as sole traders or partnerships, any liabilities incurred are likely to be in the name of those individuals. Obviously, any liabilities incurred or losses resulting from a Year 2000 problem would have a profound effect on such people.

For a limited liability company the situation is slightly different. The company is seen as a separate legal entity and the people running it would not normally incur personal liabilities on behalf of that company. However, this is not always the case and those expecting to hide from a Year 2000 problem behind the limited liability of such a company should beware. Failure by directors of a company to address a Year 2000 problem may still cause them to incur personal liabilities in a number of different ways:

- Existing legislation imposes reporting requirements on a company, which could include disclosure of a Year 2000 problem. A company is required to keep accounting records, to prepare and present financial reports and, in most cases, to have the financial reports audited. The Corporations Law in Australia sets out penalties for which every director may be liable for failing to comply with these requirements.
- These financial reports must comply with generally accepted accounting practice, which includes reporting items of 'material' importance. A materially important item is one likely to influence the users of a report in making decisions or assessments. A Year 2000 problem would certainly fall into that category due to the estimated costs of review, assessment and correction, and because of the potential disruption to a business that fails to become compliant.
- Failure to comply with reporting requirements or to address the Year 2000 problem may also constitute a breach of certain directors' duties. An example is the duty of care. Failure to plan for and prevent a known problem causing interruption of business and loss to the company could be seen as breaching this duty of care. This could result in a claim against the director by the shareholders or other directors for loss to the company, with the inevitable legal costs to follow.
- If a director knows that the company faces a Year 2000 problem that could result in its becoming insolvent with loss to the creditors and it continues to trade, this could amount to 'insolvent trading'. A director who indulges in insolvent trading may be subjected to a civil penalty and personal liability to pay compensation for debts incurred by the company.
- Failure to alert interested parties to a substantial Year 2000 problem may even amount to a criminal offence. It is an offence to make false or misleading statements or omissions that make information misleading.

This could include omission to mention a Year 2000 problem when reporting on the position of a company. Each member of a board of directors with the requisite knowledge who signs and authorises the statements would be liable.

The news is not all bad

Directors will be in a strong position to defend potential liabilities related to the Year 2000 problem if they are able to show that they:

- took steps to educate themselves about it;
- ensured that a detailed plan was developed to handle it and that sensible steps were implemented towards a viable solution; and
- took all reasonable and proper steps to ensure that reporting requirements were complied with.

ACTION POINTS

13 Do you need to disclose your Year 2000 problem in your financial reports?

14 Does your business have a Year 2000 problem that is serious enough to bring about a charge of reckless trading?

15 Are there parties interested in the business, such as potential purchasers or shareholders, to whom you should be disclosing the problem?

16 Have you documented and taken all reasonable steps towards protecting the business against a potential Year 2000 problem?

NOTES

1 The material in this chapter has been provided by Craig Jones, B. Com., LL.B., LL.M (Lond).

13 CHAPTER

Who is accountable for protecting your organisation?

The buck stops at the top

As we have seen in the previous chapter, owners, directors and managers of private-sector companies are accountable for protecting their organisations from major threats. In the government sector, the OGIT has issued guidelines and checklists against which all organisations will be assessed for compliance through the Australian National Audit Office (ANAO). So, if you are accountable in that way, you cannot evade your responsibility for ensuring that the threat is assessed and dealt with correctly.

Delegate, don't abdicate

Companies and other organisations that are subject to audit will increasingly find themselves being assessed for evidence that their Year 2000 exposure is being properly managed. This is one route by which boards of directors, for example, are first learning about the problem and their accountability for managing it. Their understandable first reaction often is to dump the responsibility for dealing with it on to whoever in the organisation is responsible for the computers. But they need to be thinking more broadly than that because, as we have seen, the problem can occur anywhere, not just in the conventional computer systems. The problem needs to be addressed from a level where the attention of the whole organisation can be mobilised, not just one specialist part of it.

This doesn't mean that if you are the boss you have to do all the work yourself. You are likely to need to delegate the technical aspects to people with the appropriate skills (or liability) for diagnosing the exposure and fixing it. In that sense, you may well be looking to the supplier of the systems or equipment to remedy any occurrence of the problem for you, depending, of course, on what is implied in your contracts with them.

It is certainly reasonable to look to your suppliers for help. Indeed, they may be the only people who can provide this assistance. But realise that they may be just as worried as you are, or even more so, and not just about the problems you are facing.

You and your suppliers are in this together

It will probably be most effective from your point of view to take a positive stance towards your computer and equipment suppliers and make it as easy as possible for them to help you and themselves.

It is entirely understandable that you may feel very aggrieved towards them for having provided you with items that may contain this time-bomb. Tempting though it might be to wave writs around, if only to find someone to blame for this mess, in point of fact you are very dependent on these suppliers to help clean up the mess; in many cases they are the only people who can. So, as was pointed out at an Azimuth Year 2000 Think Tank recently, taking the legal route is like arguing over whose end of the boat the hole is in! There is a real risk that you and your suppliers will both sink if you don't cooperate.

They are likely to be worried about their own risk, both as suppliers of problems to people like you and also as suppliers of solutions to those problems. It may take a while to get them from 'Well, we used what we considered was generally accepted good practice in our industry at the time we developed this for you', and perhaps 'We now recognise that what we delivered will cause you problems related to the Year 2000', to 'But we are able to say that the work we propose to do now will definitely put the problems right according to your definition of Year 2000 readiness', let alone 'We will provide this work under our existing maintenance contract' or 'Our charge for doing this work will be ____'. Be patient, even though time is pressing!

Don't shoot the messenger

Another route by which the organisation and its top people can first become aware of the problem is as a result of someone within the organisation, most often the person who is in charge of the computer systems, raising the matter. This is a hard thing to do convincingly and successfully and can carry a price for the individual concerned.

> **Says the chief executive:**
> So, Ms Information Systems Manager, you are telling me that I, not just you, have this very major problem:
>
> - It's going to cost a lot to fix, but you don't know how much.
> - You've been aware of it for a long time, but you're only bringing it up now.
> - If I don't spend the money, we may go out of business.
> - If I *do* spend the money, any other benefits that I receive will probably not be enough to give me a positive return on the investment.
> - Come what may, all the work has to completed by 1 January 2000.
> - It is likely to take up all our resources so all our other projects will have to be delayed.
> - On top of this, you say there is no guarantee that we'll survive at the end of all this anyway because even if you deliver on time our suppliers quite likely won't and our customers could all go belly-up.
> - And finally you say that you're not sure that we'll be able to solve all our own problems in time, anyway.
> - Well, let me tell you, that last bit is the only part of this whole preposterous story that I believe. Why? Because I've never met one of

> you computer people yet who was able to deliver anything on time, to specification and within budget. Get out of here! Next, please!

Not a particularly good start to a shared approach to solving a shared problem!

It is quite likely that what the courageous Ms Information Systems Manager is trying to get across is the best possible advice the Chief executive officer could be receiving. Unfortunately, relations between an organisation and its computer people are not always as good as they could be.

To solve the Year 2000 problems, the people who know the business and the people who know the technology need to work together. The accountability has to be shared. Revisiting past neglect by one, or past failures by the other, isn't going to help at all.

ACTION POINTS

1. **Who is accountable for ensuring that your organisation handles its Year 2000 problem properly?**
2. **What are you going to do to ensure that you can work on this problem as a team?**

14 CHAPTER

How to beat the looming skill shortage

There are probably not enough qualified people in Australia to repair all of our problems. Computer industry recruitment firms have predicted a ‘tidal wave’ of demand for Year 2000 technical skills in Australia during the next two years. Certainly, there are not enough resources around the world to repair all the problems globally.

We will have to look at other remedies, such as replacing our systems and equipment with new products, using automated repair tools (if they are available), importing skills from overseas or exporting the work overseas (for example, to South Asia), simplifying our business processes or discontinuing some lines of business. Some of these remedies may also be demanding on resources; in some cases, the same pool of resources that the repair people would come from.

Because the supply of skills is limited, its price will rise: for some types of skills this is already happening. Increases in the hourly rates of some types of technical personnel of between 6 and 10 per cent per *month* are being reported in one major centre. The lesson is: get in early! Understand that the greatest single work task will be testing that the remedies work and the business still runs as before. This is likely to be at least 50 per cent of the total effort. And the technical people will continue to be required to fix all the problems that the testing throws up.

The testing itself has to be well planned and executed, and only people who know what needs to be tested and can tell if the business is still functioning correctly should work on it. Testing will therefore place heavy demands on the staff of your organisation and this is on top of what they already do, unless some of that can be deferred.

It is my view that, even in Australia and assuming that we grasp this problem quickly, thorough testing is unlikely to be carried out in every case. The result of this is that there will be many unexpected manifestations of the problem after 1 January 2000. Indeed, for the first decade or so of the next century we will be blaming everything that goes wrong on the Year 2000, just as 20 years ago we blamed everything that went wrong on 'the computer'. In many situations in the larger countries of the developed world, thorough testing is not going to be feasible in the time that is left and serious failures are inevitable.

One strategy to think about is identifying temporary staff to bring in to run the business while the business people do the testing. An associated problem will be how to retain the services of your key personnel through to the end of your Year 2000 program given that some of them may possess skills for which other employers would pay a lot of money in this country and even more overseas.

By late 1999 it is unlikely that there will be supplies of any kind of staff, technical or temporary, to draw on at any price. So get on with it now: don't leave it until it is too late.

ACTION POINTS

1 **What are you going to do to ensure that you retain the services and skills of your own people until you no longer need them for Year 2000 work?**
2 **What are you going to do if you can't keep them?**

15 CHAPTER

What should you do now?

First, accept that this is a real issue for you and that you are running blind until you check it out.

Second, fix in your mind that this is a risk management problem that you can understand, not a technical one that you can't. There is no 'rocket science' involved, but you will need to manage the problem very carefully and thoroughly, no matter how large or small your organisation is.

Third, go through your responses to the action points contained in this book. That will give you all the awareness of your potential problem that you will need.

Fourth, *start now!*

Awareness, diagnosis and implementation

You have now accepted that you may have some problems to face, so your *awareness* is established. Now you need to:

- *Diagnose* the extent of your problems and plan how to fix or evade them.
- *Implement* your Year 2000 'fix or evade' plans and so solve your problems.

However, you should, as early as you can—perhaps even before you have started the process at all—think seriously about the possibility that you may not be able to complete all that will need to be done in the time available. On a global basis we know that there is too much work to do. This may apply in your case.

If at any stage in this diagnosis and implementation process, even right now at the outset, you feel that you may not be able to get all the work done in time, then you need to make appropriate decisions. One option is to throw more money and resources at the problem, but this may not be practicable or make business sense. Another option which you should consider is a process called *triage*.

Triage[1] is a French word and in this context it means having a hard look at your business and identifying, in the light of your expected Year 2000 exposure, those things that you do that are critical to your survival as an organisation. This is not a time-consuming activity but it needs a hard-headed approach and can be aided by some 'what iffing' ('*what if* this process fails completely?'). You made a start on this at the end of Chapter 1.

You then concentrate your Year 2000 diagnosis and implementation efforts on those processes that are mission critical, rather than on every process in the entire organisation. You will immediately simplify your Year 2000 problem and maximise your chances of staying in business after 1 January 2000, albeit with some pain in the parts of the business that you have chosen not to deal with.

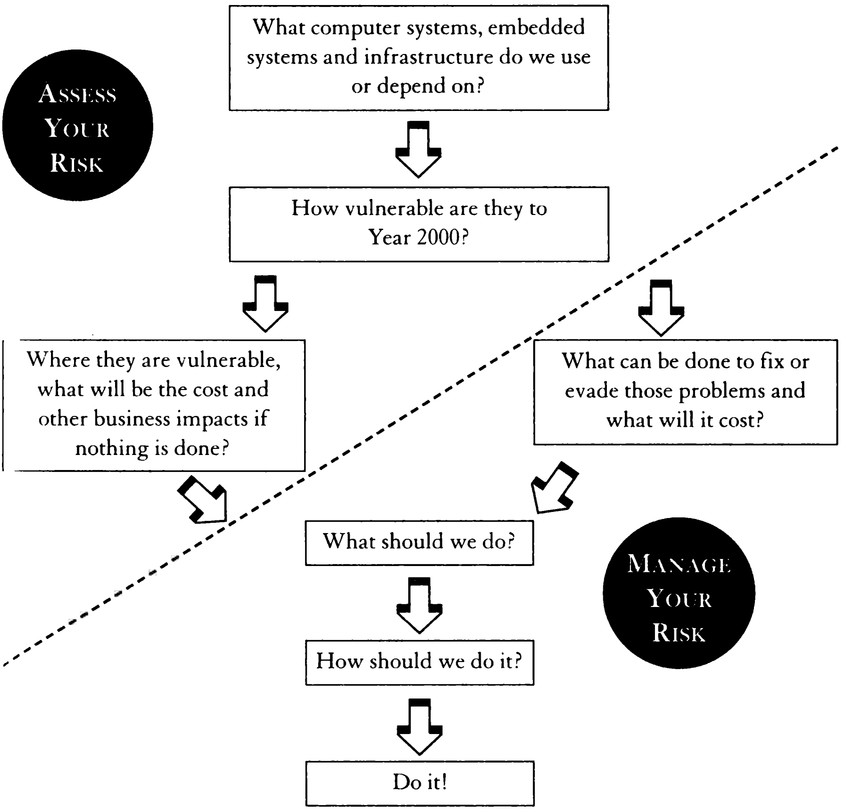
The benefits of early *triage* have already been demonstrated by some large organisations that have carried out an exhaustive inventory and risk assessment only to discover at the end of it that they are looking at too much to be accomplished in the remaining time available. So they have embarked on *triage* at that point. Had they prioritised at the outset, they would not have wasted time gathering inventory and assessing exposure for items that were not mission critical. Those organisations have lost valuable months that they will never be able to recover. Of course, these *triage* decisions can only be made by those who are responsible for the organisation, and they need to be very brave or very frightened (or both) before they can do so.

Whether you decide to work on your entire possible exposure to the Year 2000 or just on your critical business processes, diagnosis and implementation will involve the same steps.

Diagnosis essentially involves assessing your risk, and *implementation* is managing that risk. Although the two are separate processes, they can overlap in time, as shown in the diagram below.

It is likely that you will still be identifying some items of inventory and assessing their exposure to Year 2000 long after you have investigated and decided on the options for remedying the Year 2000 problems in some other items. In other words, don't allow yourself to become bogged down in one step of the process before moving on to the next. A number of organisations have fallen into that trap and have lost a lot of time as a result. We have to remember that we are probably up against the clock all

WHAT ARE THE KEY QUESTIONS?


What computer systems, embedded systems and infrastructure do we use or depend on?
ASSESS YOUR RISK
How vulnerable are they to Year 2000?
Where they are vulnerable, what will be the cost and other business impacts if nothing is done?
What can be done to fix or evade those problems and what will it cost?
What should we do?
MANAGE YOUR RISK
How should we do it?
Do it!

through this activity and must work as efficiently as we can. Speed is of the essence, so we have to push on wherever and however we can.

Assessing your risk (diagnosis)

You need to do some things immediately.

Set up a structure

No matter how small your organisation or your Year 2000 problems appear to be at the outset, set up some kind of top-driven structure for managing them.

Appoint a manager

Think hard about how you are going to manage the process over the next twenty-one months or so. Can you manage it yourself or do you need to appoint a Year 2000 program manager? Either way, there needs to be a single point of accountability for the entire process to ensure that nothing falls down the cracks and gets missed.

Encourage participation

Get everyone in your organisation thinking about the issue and how it could affect them. You may need a formal internal communications plan to enable this to happen.

Prevent further outbreaks

Take the necessary steps to prevent any further introductions of the problem. That means ensuring that suitable clauses are in contracts for purchases, as described in Chapter 12. It also means setting appropriate standards for any software development work being undertaken by your own people or by an outside supplier for you.

Establish an inventory tool

The most important step in managing the process is to design and set up an inventory tool of some kind to record all the information about each item (system or piece of equipment) so that you can be sure you know its Year

2000 status and can manage any remedial work through to a successful tested conclusion.

Even if your organisation is very small, you should still record the inventory on paper and use that as a tool for managing the process thereafter. Don't trust to memory. It is safe to assume that you will find the job more complicated than ever seemed possible at the outset.

If your inventory is going to involve more than a couple of dozen items, you should think seriously about recording it on some kind of automated tool such as a spreadsheet or database. The form on the opposite page provides an example of what you might need, though you will need to tailor the particular categories of information to your own circumstances.

Having completed these initial tasks, there are three actions/processes that you should pay attention to in order to complete your risk assessment.

Identify every conceivable location for the problem

Once you have decided on your inventory tool, the next thing to do is to start to gather your list of every conceivable location for the problem, inside your own organisation and outside (where you could be affected), and record it. You may want to design a simple questionnaire for this purpose so that the set of information you obtain is consistent and as complete as possible.

Your asset register, if you have one, may be a useful source of inventory information. However, if the register has not been well maintained, it may be more trouble than it is worth to use it for this purpose.

Gather the necessary information about your exposure

Now start to assess the extent to which each inventory item is actually affected by the Year 2000 problem. In most cases your first port of call for this information should be the supplier of the item in question. Here again, you may wish to design a questionnaire or letter to be answered by the supplier for each item. In it you should detail:

- the name of your firm;
- the name of the item/s (equipment, program, etc);
- the questions you want answered; and
- where and when to send the reply.

Item	Category	Business owner	Age of Item	Supplier	Year 2000 status	Evidence	Time Horizon to Failure	Business Plans	Business criticality	Remedial strategy	By	Test by	OK	Comments
Financials	Software	Accountant	1985	In-house	Not ready	Code check	31/12/98	None	High	Replace with package	30/06/98	31/09/98		
Payroll	Service	CEO	Since 1992	ABC Bureau	Ready	Bureau statement of compliance			High	Test, change bureau if necessary			Yes?	Check anyway
Point of sale	System	Shop	Various	XYZ	Not ready			Replace mid-1998	Medium	Replace		31/12/97	Yes	
PCs (13)	Hardware	Various	1997	PC co	Ready	Warranty			Medium		31/05/98	30/06/98		PC Co is a leading supplier
PCs (8)	Hardware	Various	1993	Koala	Not ready	Age	31/12/99	None	Low	Replace	31/07/99	31/09/99		Might make business sense to replace earlier
Alarm	Hardware	Shop	1990	Defunct	?				Medium					Supplier now out of business, replace rather than take the risk?
etc														

Sample simplified Year 2000 inventory form

The information you are seeking is:

- Is this item Year 2000 ready? (You may decide to include the definition of Year 2000 conformity provided in Chapter 4 to make it absolutely clear what you are expecting.)
- If yes, what is the basis for that statement?
- If no:
  - When is it expected to fail? (What is its Time Horizon to Failure?)
  - What does the supplier suggest should be done to remedy the situation?

You will need locations in the inventory record for each item in which to enter such information as: who the questionnaire was sent to, when it was sent, what the response was, whether you accepted it or not, the Time Horizon to Failure, and so on. For internally developed systems and equipment you will ask similar questions but perhaps in a different format designed for internal use.

In each case where you find that you really have a Year 2000 problem to deal with, you will need to understand your legal situation (see Chapter 12).

Assess the implications

The final step in assessing your risk is to assess what each of the Year 2000 exposures that has been identified means for your business. This is likely to involve further discussions with the people who use or are accountable for the use of the items affected. The objective will be to establish:

- the role each item plays in the organisation; and
- the business significance of this role: is it mission critical, of some importance or just nice to have?

For each item, all of the information obtained should be recorded in summarised form in the inventory record. Having assessed your risk from Year 2000 to the extent possible, without spending too much time on it, you can set about managing it to best advantage.

Managing your risk (implementation)

What can be done and what should we do? First, you have to find out what your options are for fixing or evading each occurrence of the problem.

Whether you decide to concentrate on the mission-critical processes as the result of *triage* or feel that you have time to look at every process within your organisation, managing your risk requires that you must look at every item in the inventory where it is possible that the Year 2000 will have an impact. That is, you need to concentrate on every item where you don't yet know for sure that there won't be an impact. These are the things you need to do:

1. Find out what your options are for fixing or evading the problems. Primary sources for this information will be your suppliers and your own staff. Other possible sources of information are indicated in Chapter 16.
2. Establish whether the normal course of business events (replacements, obsolescence, new products, new markets) will save you to some extent. Will the item no longer be important or even still in existence before the problems occur? Do you plan to replace it anyway?
3. In all cases, prioritise what you are going to do in terms of the risk to your business. You need to understand that priority here is about what is most important, not about what is done first; just so long as your plan allows you to complete all the work that you have decided to do in time. Your priorities should be driven primarily by the magnitude of the risk to your business—but within that, prioritise in this sequence:
   - (a) Look after the risk in your own systems and equipment and, first of all, your areas of mission-critical risk—in part because these will probably involve the greatest effort on your own part.
   - (b) Address your risk from your suppliers and customers next, because it is up to them to fix their problems and you may have opportunities to switch to different ones if you have to.
   - (c) Finally, look at your infrastructure risks, such as power, telephones and the like, where there is probably little you can do to help, it is all up to the organisations providing them, and there may not be too many other options available anyway.

Having decided what you are going to do, you can then start to make plans for doing it.

Make an action plan

With your inventory to hand, draw up a plan covering everything you have decided to do. You need to work out, for each item, when work has to start, when it must be completed by, and who is responsible for doing the work. Enter these key details into the inventory record so that you can monitor what is going on. In making your plan, bear the following points in mind.

Testing will be the biggest task

You need to allow at least as much time for testing the remedies as you do for all of the other Year 2000 activities combined—remedying one set of problems nearly always introduces others. You need to be sure, not just that each item is now Year 2000 ready and works properly, but that all items together run the way you expect them to.

Contingency plans

Things may not go to plan, often because of factors outside your control. Tasks may fall behind schedule and not be recoverable. For this reason you need contingency plans. These will identify what you will do for any key item if it becomes clear that your preferred remedial actions aren't going to work. Since contingency actions will also involve time and other resources, you need to calculate a contingency action date in each case: the date when the planned alternative for a task that is late has to be started.

For each of your mission-critical items you need to decide your contingency plan at the same time as you set up your plan for remedying the problem, so that you aren't left high and dry if your preferred remedy fails.

Now do it!

Implement your action plan! Monitor your progress as you go. You can use the Year 2000 Good Practice Checklist at the end of this chapter to help you do this.

Be prepared to change tack

Don't be afraid to change your plans in the light of progress. If some things go more slowly than expected and you find that new tasks have to be accommodated, then so be it. It is not a sign of weakness to respond to life's realities, but it could be considered a sign of pig-headedness if you refuse to adjust until it is too late!

While you're about it

Check out your suppliers and customers

Consider approaching your suppliers and customers to see how they are addressing the Year 2000 issue (if at all). It is up to them to fix their problems, but if you find that they are not you may want to consider transferring your loyalties. Consider also, as we discussed earlier, that offering them the benefit of your experience on the matter may well be in your best interests in the long run.

Watch for new developments

Keep an eye on Year 2000 progress in general to see if new developments and techniques could help you.

Accentuate the positive!

Look for opportunities for your organisation as a result of the Year 2000 impacts on others. You will probably be ahead of the bunch in your markets and your sector because of the thorough and orderly way you are handling your risk. Competitive advantages should therefore open up for you, whatever the state of the world in 2000 and beyond. Look for them! (You started thinking about this at the end of Chapter 2.)

And finally—plan for business continuity, come what may

You may not get it all right, despite your best efforts. What will you do if the unexpected does happen and a key process breaks down as a result of the transition to the Year 2000? Quite possibly you won't be able to do anything very effective if you haven't thought about it until then. But if you have thought it through and made some preparations—for your vital processes at least—you can just switch to plan 'B'; an alternative way of doing things which will keep you going. This is the last precaution which you can probably take—and is well worth doing.

Here, again, there are some pointers to bear in mind:

- In your planning for business continuity don't get embedded in detailed speculation about areas of risk that you may have missed. Just ask yourself, for example, how will we pay our people if the payroll process fails? This isn't too hard a problem to solve—perhaps by using a manual process—if you have thought it through and prepared for it in advance. It wasn't so long ago that we were all paid in cash.

- Don't just plan the alternative—test it out. It may not always be practicable to do a full test but if you *can* test, do so.
- Understand that plan 'B' has to be a *different* way of doing the process. An identical back-up process, of the kind which is often used for essential computer systems to guard against the more conventional types of disaster, won't help at all. If your normal process suffers Year 2000 problems, your back-up will suffer the same problems if it is identical to the normal one.

Consider the virtues of not throwing out, at this stage, old equipment which doesn't involve electronics. And think hard again about the virtues of manual back-up systems. *People* don't suffer from Year 2000 problems! And, as quoted earlier, 'people and organisations are extraordinarily capable', especially when given the chance to be so.

Year 2000 Good Practice Checklist

This checklist was developed by the Y2K Committee, a New Zealand group set up by the Information Technology Unit of the Ministry of Commerce and ITANZ, an organisation representing information technology suppliers. The committee's role is to raise awareness of the issue.

You can feel confident that you are managing your risk when you can answer 'yes' to all the following questions.

Ten questions for everyone responsible for an organisation or business[1]

1. Do we have complete inventories of our information systems and anything else that might contain computer chips?
2. Do we know the extent of our Year 2000 problem and the likely impact on our business?
3. Do we have a program in place for raising awareness about the problem?
4. Have we taken steps to ensure that the Year 2000 problem will not arise in any new systems we introduce?

5 Do we know our risk from the Year 2000 problems of the other organisations and infrastructures on which we depend?
6 Do we know our risk from the impact of our Year 2000 problem on them?
7 Do we have contingency plans that cover our own and others' failures to fix the problem?
8 Do we understand our legal position under our contracts with our suppliers and customers?
9 Do we know when the Year 2000 problem did or will first strike us?
10 Have we drawn up a program of remedial work that reflects our business priorities and does it have enough funds, time and other resources?'

To ensure that you stay on track you should answer these questions honestly and regularly (say, every month) between now and the successful completion of your Year 2000 work.

NOTES

1 *Triage* is a military/medical term originally used to describe a process by which casualties could be most efficiently handled in a battlefield situation. On initial examination the casualties were allocated to one of three groups: those who were going to get better anyway, those who were going to die anyway, and those for whom medical treatment could make a vital difference. The first two groups would be made as comfortable as possible, and the limited medical resources and time would be concentrated on the third group.

2 Adapted from 'Questions for Directors and Chief Executives', Y2K Committee, 1996.

16 CHAPTER

Where to obtain further help

The aim of this book is to provide a basic understanding and enough information to enable an organisation to get started on a Year 2000 program. More information is likely to be needed in every case.

Places to look for additional information or assistance include:

- Your technical suppliers of software, hardware, equipment and support services.
- Your own staff.
- The documentation for your systems and equipment.
- The Internet—useful sites include:
    - http://www.datamation.com/PlugIn/workbench/yr2000/year.htm
    - Peter de Jager and links to much more are at http://www.year2000.com
    - http://www.computerworld.com/year2000
    - a bibliography of published Year 2000 material is at http://www.deweerd.org/year2000/biblio
    - http://www.aiia.com.au/year2000.html
    - for coverage of current global Year 2000 practice, Gartner Group is at http://www.gartner.com
    - for embedded systems, look at the U.K. Institute of Electrical Engineers' site at http://www.iee.org.uk/2000risk
- The 'bible' for electronic chips and how they function (but not their

Year 2000 aspects as yet) is at http://infopad.eecs.berkeley.edu/CIC/archive/cpu_history.html

- Australian state government sites are at:
  - NSW http://www.nsw.gov.au
  - SA http://www.sacentral.sa.gov.au/agencies/clits/y2kpage.htm
  - WA http://www.wa.gov.au
  - NT http://www.nt.gov.au
  - ACT http://www.act.gov.au
  - Qld http://www.qld.gov.au and http://www.ipb.qld.gov.au
  - Vic http://www.vic.gov.au
    http://www.vic.gov.au/ocmpol/12A.html
    Tas http://www.tas.gov.au
  - A national Y2K Web site—all Australian governments working together—is currently being established at http://www.Y2K.gov.au
- Year 2000 service providers. The OGIT has a Year 2000 Web site that provides information about these at http://www.ogit.gov.au/index2.html
- Your own trade press.
- Media computer pages and specialist magazines.
- A thorough six-volume series of manuals entitled *Tackling the Year 2000* has been produced by the CCTA (Central Computer and Telecommunications Agency) in Britain.

Appendix: Review your organisation

This appendix is designed to be used with the Action Points in each chapter to review your organisation's readiness for Year 2000. Write your responses in the spaces provided.

Chapter 1

1 List the critical business processes for your organisation—the ones that must not fail if you are to stay in business.

2 Do you know (not just think you know, but really know) the extent of your organisation's risk from the Year 2000 problem?
YES ☐ NO ☐

3 What are the processes in your organisation in which you could have Year 2000 problems before 1 January 2000 if they are not Year 2000 ready?

Chapter 2

If you knew that your organisation was going to be ready for Year 2000 in time and that some of your competitors were not going to be, how could you turn that situation to your advantage?

Chapter 3

Cross out any of the following areas if there is no way in which it could contain a Year 2000 risk to your organisation:

- conventional information systems
- personal computers
- applications running on personal computers
- data networks
- embedded chips in equipment
- infrastructures like banks, telecommunications, transport
- your suppliers
- your customers
- your other stakeholders
- your industry

Chapter 5

1 Make a list of the conventional information systems your organisation uses.

2 Do you know the extent of the Year 2000 exposure in those systems?
YES ☐ NO ☐

3 Which systems support the processes that are essential for you to continue in business?

Chapter 6

1 Make a complete list of your PCs (summarise if you have a lot of them).

____

____

____

____

____

____

2 Do you know when each one was bought new?
YES ☐ NO ☐

3 Do you have a policy of regular replacement for PCs?
YES ☐ NO ☐

4 Will every PC purchased new earlier than 1996 (1997 if it is not a 'name' brand) have been replaced before 2000?
YES ☐ NO ☐

5 Are you running on the latest versions of the software you use?
YES ☐ NO ☐

6 Do you have it in writing from the supplier that your applications software is ready for the Year 2000?
YES ☐ NO ☐

7 Are you confident that if you or your PC users have developed applications to run on them, they have always used four-digit years and never two-digit years?
YES ☐ NO ☐

Chapter 7

1 Using the table of potential locations for embedded chips as a guide, draw up a list for your organisation. Then, for each item, think about the impact on your business if it failed at or before 1 January 2000.

____

____

____

____

____

____

____

____

2 Which items couldn't you live without?

3 How long would it take to replace each of the essential items, if you had to, because it was incurably afflicted by the Year 2000 problem?

4 If your premises are leased, is Year 2000 readiness for the lifts, security, environmental controls, roller doors, fire safety, irrigation and other equipment included in the contract?
YES ☐ NO ☐

5 Would it be possible to test any equipment that you feel may have the problem as part of the next regular maintenance cycle?
YES ☐ NO ☐

Chapter 8

1 In terms of your business survival, who are your critical suppliers?

2 Could you find alternatives to those suppliers if you had to?
YES ☐ NO ☐

3 If yes, how long would that process take?

4 Think about those critical suppliers: are there things that you could do to help ensure that they are Year 2000 ready?

Chapter 9

1 What would be the impact on your business if 1 per cent or 5 per cent or 20 per cent of your typical customers failed at around the same time?

2 How many of your customers, do you think, are even aware of the Year 2000 problem?

3 How many, do you think, are doing something about it?

4 Does this particularly matter to you? Are you in the happy position that your customers are extremely unlikely to be affected by Year 2000 or, if some of them fail, you will be able to find others?

5 If it does matter to you, are there things you could do to encourage them to address the issue in time?

____

____

____

____

____

Chapter 10

1 Make a list of your critical infrastructure suppliers.

____

____

____

____

____

____

____

____

____

2 Is your industry:

- Dependent on dates and large amounts of information (eg banking)?
  YES ☐ NO ☐
- Highly networked (eg telecommunications or fast-moving consumer goods)?
  YES ☐ NO ☐
- Dependent on applications written by users on personal computers (as in some parts of the finance sector)?
  YES ☐ NO ☐
- Dependent on legacy systems, either your own or a business partner's (eg manufacturing, air transport, insurance)?
  YES ☐ NO ☐
- Dependent on automated process control (eg manufacturing, publishing)?
  YES ☐ NO ☐

3 On balance, which of these best describes the Year 2000 factor?

	For your industry:	For you:
■ a threat	☐	☐
■ an opportunity	☐	☐
■ a balance of threats and opportunities	☐	☐
■ no real impact either way	☐	☐

4 What is the current level of Year 2000 activity in your industry: Everybody's on to it? Nobody even knows about it? Somewhere in-between?

5 Is Year 2000 being specifically addressed in a constructive way (or at all) in your trade publications, seminars and the like?
YES ☐ NO ☐

6 Are you aware of other players in your industry that are already working to remedy the problem? List them.

7 Do you know or can you find out what they are doing?
YES ☐ NO ☐

Chapter 11

1 Can you see potential advantages for your organisation as a result of Australia (and you) handling Year 2000 well? If yes, what are they?

2 What potential advantages can you see for Australia if organisations like yours handle it well?

Chapter 12

1 Make a complete list of the agreements relevant to your business.

2 In any case where you don't have a signed agreement, do you have relevant background correspondence that addresses the legal relationship between the parties?
YES ☐ NO ☐

3 Is any step you intend to take to prevent a Year 2000 problem prohibited under agreements relevant to the product you are working on?
YES ☐ NO ☐

4 Do you require the consent of other parties to alter the product, and what form should this consent take?

5 What could be the consequences of failing to comply with these agreements?

6 Do all your staff who may enter into purchase or sale agreements on your behalf know that the Year 2000 problem should be addressed?
YES ☐ NO ☐

7 In the cases of both sale and purchase agreements, are there warranties that the product or service is Year 2000 compliant and is the term 'compliant' clearly defined?
YES ☐ NO ☐

8 How is the Year 2000 compliance of the product or service to be tested?

9 Are there legal barriers to your access to the basic components of a product required to correct a Year 2000 problem yourself if need be?
YES ☐ NO ☐

10 List any major barriers.

11 Is the potential liability of the other party adequate to cover any potential loss you may incur due to a Year 2000 problem?
YES ☐ NO ☐

12 List any major inadequacies.

13 Do you need to disclose your Year 2000 problem in your financial reports?
YES ☐ NO ☐

14 Does your business have a Year 2000 problem that is serious enough to bring about a charge of reckless trading?
YES ☐ NO ☐

15 Are there parties interested in the business, such as potential purchasers or shareholders, to whom you should be disclosing the problem?
YES ☐ NO ☐

16 Have you documented and taken all reasonable steps towards protecting the business against a potential Year 2000 problem?
YES ☐ NO ☐

Chapter 13

1 Who is accountable for ensuring that your organisation handles its Year 2000 problem properly?

2 What are you going to do to ensure that you can work on this problem as a team?

Chapter 14

1 What are you going to do to ensure that you retain the services and skills of your own people until you no longer need them for Year 2000 work?

2 What are you going to do if you can't keep them?

DEATH.

TAXES.

2000AD.

As we approach the new millennium, three things in life are certain. We can't help with the first two. But fortunately, Azimuth, can assist with the latest addition.

Azimuth is Australasia's largest independent business and information management consultancy. Our experienced consultants can guide your organisation toward total readiness for the year 2000, by carrying out appraisals of the likely impact of the two digit year problem on your business, and planning and managing a programme of remedial actions tailored to your needs.

To find out more, phone us today. Think of it as the first step towards having a little less certainty in your life!

Azimuth

AZIMUTH CONSULTING AUSTRALIA PTY LTD

CANBERRA

Telephone 02-6260 3443 Facsimile 02-6260 3362

Offices also in Auckland, Wellington, Christchurch and Manila

ACN 065 458 317

AA&D

DIGITAL ARMAGEDDON 2000

How to stop the Millennium bug before it stops your business

For every citizen of the twentieth century who needs to be able to function in the twenty-first!

A major international crisis threatens to destabilise the world at the turn of the century. When 1999 moves to 2000, the transition to the new century may be mishandled by many older computer systems as the date appears to move backwards from '99' to '00'. This may result in computer malfunctions on a global scale.

The problem will not only occur in conventional computer systems, but also in any device with embedded computer chips such as cash registers and lifts, security systems, telephone systems and the hundreds of other modern business tools we take for granted every day.

Digital Armageddon 2000 is a practical, easy-to-understand guide to this potential crisis. Written in non-technical, plain English, it provides sound advice on how the problem may affect you and your business, and on how you can manage the risks and achieve a smooth transition to the next millennium. It also shows how to recognise and take advantage of the opportunities that the Millennium bug may offer.

John Good is a Senior Consultant at Azimuth Consulting, advising a variety of major organisations on the management of the Millennium bug issue. He is also a media commentator as well as a member of the New Zealand Y2K Committee—brought together by government and industry sectors to raise awareness of the issue.

ISBN 0-7248-0318-1

9 780724 803187

PRENTICE HALL

DIGITAL ARMAGEDDON 2000

JOHN GOOD

PRENTICE HALL